

May 2018

G r e e c e

National Risk Assessment ML/TF

CONFIDENTIAL

Table of Contents

INTRODUCTION.....	17
1. RISK ASSESSMENT	19
1.1. Overall money laundering risk in the jurisdiction	19
1.2. Sector risks	19
2. THREAT	21
2.1. Summary.....	21
2.2. Threat from predicate offenses	22
2.2.1. Drug Trafficking	22
2.2.2. Corruption	23
2.2.3. Crimes against property	24
2.2.4. Financial crimes	25
2.2.5. Smuggling of migrants and refugees.....	28
2.2.6. Tax evasion – Tax offences.....	29
2.3. External threat level	30
2.4. Threat level per sector	31
2.4.1. Banking Sector.....	31
2.4.2. Life Insurance Company Sector.....	31
2.4.3. Capital market sector	32
2.4.4. Other financial institutions.....	33
2.4.4.1. Money remittance providers	33
2.4.4.2. E-money issuers.....	33
2.4.4.3. Currency exchange offices	34
2.4.4.4. Factoring companies	34
2.4.4.5. Financial leasing companies	34
2.4.4.6. Credit companies.....	34
2.4.5. Non financial sector.....	35
3. NATIONAL VULNERABILITY.....	37
3.1. Summary.....	37
3.2. National ML combating ability factors	37
3.3. National sector vulnerability	40
3.4. National Vulnerability.....	41

3.5.	National ML combating ability factors	43
3.5.1.	Quality of AML policy and strategy	43
3.5.2.	Effectiveness of ML crime definition.....	44
3.5.3.	Comprehensiveness of asset forfeiture laws	46
3.5.4.	Quality of FIU intelligence gathering and processing	50
3.5.5.	Capacity and resources for financial crime investigations (including asset forfeiture).....	53
3.5.6.	Capacity and resources for financial crime prosecutors (including Asset forfeiture).....	54
3.5.7.	Capacity and resources for judicial processes (including asset forfeiture).....	54
3.5.8.	Integrity and independence of financial investigators (including Asset Forfeiture)	55
3.5.9.	Integrity and independence of financial crime prosecutors (including Asset Forfeiture)	56
3.5.10.	Integrity and independence of judges(including Asset Forfeiture)	56
3.5.11.	Quality of border controls	57
3.5.12.	Comprehensiveness of customs regime on cash and similar instruments.....	58
3.5.13.	Effectiveness of customs controls on cash and similar instruments	59
3.5.14.	Effectiveness of domestic cooperation	60
3.5.15.	Effectiveness of international cooperation.....	61
3.5.16.	Availability of independent audit	66
3.5.17.	Level of financial integrity	68
3.5.18.	Effectiveness of tax enforcement	69
3.5.19.	Formalization level of economy	70
3.5.20.	Availability of reliable identification infrastructure	72
3.5.21.	Availability of independent information sources.....	73
3.5.22.	Availability and access to beneficial ownership information.....	74
4.	BANKING SECTOR	75
4.1.	Summary.....	75
4.2.	Banking sector overview	77
4.3.	Specific characteristics of the greek banking sector	78
4.3.1.	Capital controls.....	78
4.3.2.	Tax evasion	78

4.3.3.	Cash activity.....	79
4.4.	Banking sector vulnerability	79
4.4.1.	General AML controls.....	80
4.4.1.1.	Comprehensiveness of AML legal framework	80
4.4.1.2.	Effectiveness of supervision procedures and practices	82
4.4.1.3.	Availability and enforcement of administrative sanctions	84
4.4.1.4.	Availability and effectiveness of entry controls.....	85
4.4.1.5.	Integrity of leadership and staff	86
4.4.1.6.	Availability and enforcement of criminal sanctions.....	86
4.4.1.7.	Level of market pressure to meet AML standards.....	87
4.4.1.8.	Effectiveness of compliance function	88
4.4.1.9.	AML knowledge of bank’s staff	89
4.4.1.10.	Effectiveness of suspicious activity monitoring and reporting	89
4.5.	Product and service vulnerability.....	91
4.5.1.	Deposits of natural persons	91
4.5.2.	Deposits of legal persons	92
4.5.3.	Credit transfers.....	93
4.5.4.	Loans of natural and legal persons	94
4.5.5.	Cheques	94
4.5.6.	Private banking.....	95
4.5.7.	Trade financing.....	96
4.5.8.	Correspondent Banking.....	96
4.5.9.	Safe deposit services	97
4.5.10.	Credit cards.....	98
5.	CAPITAL MARKET SECTOR	99
5.1.	Overview.....	99
5.2.	Review of the capital market sector	101
5.3.	Capital market sector vulnerability assessment	102
5.4.	General AML controls.....	103
5.4.1.	Comprehensiveness of AML legal framework.....	103
5.4.2.	Effectiveness of supervision procedures and practices	104
5.4.3.	Availability and enforcement of administrative sanctions	104

5.4.4.	Availability and enforcement of criminal sanctions.....	105
5.4.5.	Availability and enforcement of entry controls	105
5.4.6.	Integrity of staff in securities firms	106
5.4.7.	Integrity of staff in securities firms	106
5.4.8.	Effectiveness of compliance function (organization).....	107
5.4.9.	Effectiveness of suspicious activity monitoring and reporting	107
5.4.10.	Level of market pressure to meet AML standards.....	108
5.5.	Inherent vulnerability variables	108
5.5.1.	Investment services firms.....	108
5.5.2.	Fund and asset management companies	109
5.5.3.	Receival and transmission companies	109
5.5.4.	Portfolio investment companies	109
6.	INSURANCE SECTOR	110
6.1.	Summary.....	110
6.2.	Life insurance sector overview	110
6.3.	Insurance sector vulnerability assessment	110
6.4.	General input variables	111
6.4.1.	Comprehensiveness of AML legal framework	112
6.4.2.	Availability and effectiveness of entry controls	112
6.4.3.	Effectiveness of supervision procedures and practices	113
6.4.4.	Availability and enforcement of administrative sanctions	114
6.4.5.	Availability and enforcement of criminal sanctions.....	115
6.4.6.	Integrity of staff in insurance companies.....	115
6.4.7.	Effectiveness of compliance function	116
6.4.8.	AML knowledge of staff in insurance companies	117
6.4.9.	Level of market pressure to meet AML standards.....	117
6.4.10.	Effectiveness of suspicious activity monitoring and reporting	117
6.4.11.	Availability and access to beneficial ownership information.....	118
6.4.12.	Availability of reliable identification infrastructure,	118
6.4.13.	Availability of independent information sources.....	118
6.5.	Inherent vulnerability variables (Life insurance products analysis).....	118
6.5.1.	Use of intermediaries	121

6.5.2.	Cash activity and tax evasion	122
6.5.3.	Anonymous and non-face to face use of products	122
7.	OTHER FINANCIAL INSTITUTIONS SECTOR	124
7.1.	Executive summary	124
7.2.	Other financial institutions ML vulnerability.....	125
7.3.	Inherent ML vulnerability	126
7.3.1.	Money remitters	126
7.3.2.	E-money issuers.....	128
7.3.3.	Bureaux de change	129
7.3.4.	Factoring companies	129
7.3.5.	Financial leasing companies	130
7.3.6.	Credit companies.....	131
7.4.	General AML Controls	132
7.4.1.	Comprehensiveness of AML legal framework	133
7.4.2.	Effectiveness of supervision/oversight activities	133
7.4.3.	Availability and enforcement of administrative sanctions	134
7.4.4.	Availability and enforcement of criminal sanctions.....	134
7.4.5.	Availability and effectiveness of entry controls	135
7.4.6.	Integrity of business/institution staff.....	136
7.4.7.	AML knowledge of business/institution staff	137
7.4.8.	Effectiveness of compliance function (Organization)	138
7.4.9.	Effectiveness of suspicious activity monitoring and reporting	138
8.	DESIGNATED NON-FINANCIAL BUSINESSES AND PROFESSIONS	140
8.1.	Overview of Designated Non-Financial Businesses and Professions	140
8.2.	DNFBPs vulnerability assessment	142
8.3.	Lawyers.....	145
8.3.1.	General variables.....	145
8.3.1.1.	Comprehensiveness of anti-money laundering (AML) legal framework	145
8.3.1.2.	Effectiveness of supervision / oversight activities	145
8.3.1.3.	Availability and enforcement of administrative sanctions	145
8.3.1.4.	Availability and enforcement of criminal sanctions.....	146
8.3.1.5.	Availability and effectiveness of entry controls	146

8.3.1.6.	Integrity of business/profession staff	146
8.3.1.7.	AML Knowledge of business/profession staff.....	147
8.3.1.8.	Effectiveness of compliance function	147
8.3.1.9.	Effectiveness of suspicious activity monitoring and reporting.....	147
8.3.2.	Inherent vulnerability (High)	148
8.3.2.1.	Total size/volume of the business/profession	148
8.3.2.2.	Client-base profile of the business/profession	148
8.3.2.3.	Level of cash activity associated with the business/profession.....	149
8.4.	Accountants - Tax advisors.....	149
8.4.1.	General variables.....	149
8.4.1.1.	Comprehensiveness of anti-money laundering (AML) legal framework	149
8.4.1.2.	Effectiveness of supervision / oversight activities	150
8.4.1.3.	Availability and enforcement of administrative sanctions	150
8.4.1.4.	Availability and enforcement of criminal sanctions.....	151
8.4.1.5.	Availability and effectiveness of entry controls	151
8.4.1.6.	Integrity of business/profession staff	152
8.4.1.7.	AML knowledge of business/profession staff	152
8.4.1.8.	Effectiveness of compliance function	153
8.4.1.9.	Effectiveness of suspicious A.activity monitoring and reporting.....	153
8.4.2.	Inherent vulnerability (High)	153
8.4.2.1.	Total size/volume of the business/profession	153
8.4.2.2.	Client-base profile of the business/profession	154
8.4.2.3.	Level of cash activity associated with the business/profession.....	154
8.5.	Notaries	155
8.5.1.	General variables.....	155
8.5.1.1.	Comprehensiveness of anti-money laundering (AML) legal framework	155
8.5.1.2.	Effectiveness of supervision / oversight activities	155
8.5.1.3.	Availability and enforcement of administrative sanctions	155
8.5.1.4.	Availability and enforcement of criminal sanctions.....	156
8.5.1.5.	Availability and effectiveness of entry controls	156
8.5.1.6.	Integrity of business/profession staff	156
8.5.1.7.	AML knowledge of business/profession staff	156

8.5.1.8.	Effectiveness of compliance function	157
8.5.1.9.	Effectiveness of suspicious activity monitoring and reporting	157
8.5.2.	Inherent vulnerability (High)	157
8.5.2.1.	Total size/volume of the business/profession	157
8.5.2.2.	Client-base profile of the business/profession	158
8.5.2.3.	Level of cash activity associated with the business/profession.....	158
8.6.	Pawnbrokers.....	159
8.6.1.	General variables.....	159
8.6.1.1.	Comprehensiveness of anti-money laundering (AML) legal framework	159
8.6.1.2.	Effectiveness of supervision / oversight activities	159
8.6.1.3.	Availability and enforcement of administrative sanctions	160
8.6.1.4.	Availability and enforcement of criminal sanctions.....	161
8.6.1.5.	Availability and effectiveness of entry controls	161
8.6.1.6.	Integrity of business/profession staff	162
8.6.1.7.	AML knowledge of business/profession staff	162
8.6.1.8.	Effectiveness of compliance function	162
8.6.1.9.	Effectiveness of suspicious activity monitoring and reporting	162
8.6.2.	Inherent vulnerability (Medium High)	163
8.6.2.1.	Total size/volume of the business/profession	163
8.6.2.2.	Client-base profile of the business/profession	163
8.6.2.3.	Level of cash activity associated with the business/profession.....	163
8.6.2.4.	Other vulnerable factors of the business/profession: Use of the business/profession in fraud or tax evasion schemes	163
8.7.	Real estate agents	164
8.7.1.	General variables.....	164
8.7.1.1.	Comprehensiveness of anti-money laundering (AML) legal framework	164
8.7.1.2.	Effectiveness of supervision / oversight activities	164
8.7.1.3.	Availability and enforcement of administrative sanctions	164
8.7.1.4.	Availability and enforcement of criminal sanctions.....	165
8.7.1.5.	Availability and effectiveness of entry controls	165
8.7.1.6.	Integrity of business/profession staff	166
8.7.1.7.	AML knowledge of business/profession staff	166

8.7.1.8.	Effectiveness of compliance function	167
8.7.1.9.	Effectiveness of suspicious activity monitoring and reporting	167
8.7.2.	Inherent vulnerability (Medium High)	167
8.7.2.1.	Total size/volume of the business/profession	167
8.7.2.2.	Client-base profile of the business/profession	168
8.7.2.3.	Level of cash activity associated with the business/profession.....	168
8.8.	Dealers in high-value goods	169
8.8.1.	General variables.....	169
8.8.1.1.	Comprehensiveness of anti-money laundering (AML) legal framework	169
8.8.1.2.	Effectiveness of supervision / oversight activities	169
8.8.1.3.	Availability and enforcement of administrative sanctions	169
8.8.1.4.	Availability and enforcement of criminal sanctions.....	170
8.8.1.5.	Availability and effectiveness of entry controls	170
8.8.1.6.	Integrity of business/profession staff	170
8.8.1.7.	AML knowledge of business/profession staff	170
8.8.1.8.	Effectiveness of compliance function	171
8.8.1.9.	Effectiveness of suspicious activity monitoring and reporting	171
8.8.2.	Inherent vulnerability (Medium High)	171
8.8.2.1.	Total size/volume of the business/profession	172
8.8.2.2.	Client-base profile of the business/profession	172
8.8.2.3.	Level of cash activity associated with the business/profession.....	172
8.8.2.4.	Other vulnerable factors of the business/profession: Non-face-to-face transactions with the client	172
8.9.	Land-based gambling	173
8.9.1.	General variables.....	173
8.9.1.1.	Comprehensiveness of anti-money laundering (AML) legal framework	173
8.9.1.2.	Effectiveness of supervision / oversight activities	173
8.9.1.3.	Availability and enforcement of administrative sanctions	174
8.9.1.4.	Availability and enforcement of criminal sanctions.....	174
8.9.1.5.	Availability and effectiveness of entry controls	174
8.9.1.6.	Integrity of business/profession staff	175
8.9.1.7.	AML knowledge of business/profession staff	175

8.9.1.8.	Effectiveness of compliance function	176
8.9.1.9.	Effectiveness of suspicious activity monitoring and reporting	176
8.9.2.	Inherent vulnerability (High)	177
8.9.2.1.	Total size/volume of the business/profession	177
8.9.2.2.	Client-base profile of the business/profession	177
8.9.2.3.	Level of cash activity associated with the business/profession.....	177
8.9.2.4.	Other vulnerable factors of the business/profession: Use of agents/intermediaries.....	177
8.9.2.5.	Other vulnerable factors of the business/profession: Possible anonymous use of the product in the business/profession.....	178
8.9.2.6.	Other vulnerable factors of the business/profession: Difficulty in tracing the transactions.....	178
8.10.	Online gambling	178
8.10.1.	General variables.....	178
8.10.1.1.	Comprehensiveness of anti-money laundering (AML) legal framework	178
8.10.1.2.	Effectiveness of supervision / oversight activities	178
8.10.1.3.	Availability and enforcement of administrative sanctions	179
8.10.1.4.	Availability and enforcement of criminal sanctions.....	179
8.10.1.5.	Availability and effectiveness of entry controls	179
8.10.1.6.	Integrity of business/profession staff	180
8.10.1.7.	AML knowledge of business/profession staff	180
8.10.1.8.	Effectiveness of compliance function	180
8.10.1.9.	Effectiveness of suspicious activity monitoring and reporting	181
8.10.2.	Inherent vulnerability (Medium High)	181
8.10.2.1.	Total size/volume of the business/profession	181
8.10.2.2.	Client-base profile of the business/profession	181
8.10.2.3.	Level of cash activity associated with the business/profession.....	182
8.10.2.4.	Other vulnerable factors of the business/profession: Possible anonymous use of the product in the business/profession.....	182
8.10.2.5.	Other vulnerable factors of the business/profession: Difficulty in tracing the transactions.....	182
8.10.2.6.	Other vulnerable factors of the business/profession: Non-face-to-face transactions with the client	182

8.11.	Certified Auditors - Accountants.....	182
8.11.1.	General variables.....	182
8.11.1.1.	Comprehensiveness of anti-money laundering (AML) legal framework	182
8.11.1.2.	Effectiveness of supervision / oversight activities	183
8.11.1.3.	Availability and enforcement of administrative sanctions	184
8.11.1.4.	Availability and enforcement of criminal sanctions.....	184
8.11.1.5.	Availability and effectiveness of entry controls	185
8.11.1.6.	Integrity of business/profession staff	186
8.11.1.7.	AML knowledge of business/profession staff	186
8.11.1.8.	Effectiveness of compliance function	187
8.11.1.9.	Effectiveness of suspicious activity monitoring and reporting	187
8.11.2.	Inherent vulnerability (Medium High)	188
8.11.2.1.	Total size/volume of the business/profession	188
8.11.2.2.	Client-base Profile of the business/profession	188
8.12.	Auction Houses.....	189
8.12.1.	General variables.....	189
8.12.1.1.	Comprehensiveness of anti-money laundering (AML) legal framework	189
8.12.1.2.	Effectiveness of supervision / oversight activities	189
8.12.1.3.	Availability and enforcement of administrative sanctions	190
8.12.1.4.	Availability and enforcement of criminal sanctions.....	190
8.12.1.5.	Availability and effectiveness of entry controls	190
8.12.1.6.	Integrity of business/profession staff	191
8.12.1.7.	AML Knowledge of business/profession staff.....	191
8.12.1.8.	Effectiveness of compliance function	191
8.12.1.9.	Effectiveness of suspicious activity monitoring and reporting	192
8.12.2.	Inherent vulnerability (Medium).....	192
8.12.2.1.	Total size/volume of the business/profession	192
8.12.2.2.	Client-base profile of the business/profession	192
8.12.2.3.	Level of cash activity associated with the business/profession.....	192
8.12.2.4.	Other vulnerable factors of the business/profession: Non-face-to-face transactions with the client	193
9.	ASSESSMENT OF TERRORISM FINANCING IN GREECE	194

9.1.	Intorduction.....	194
9.2.	Terrorism financing assessment.....	194
9.3.	Terrorism threat assessment	195
9.3.1.	Domestic terrorism	195
9.3.1.1.	Far left wing – Anarchist terrorism	195
9.3.1.2.	Far right wing terrorism	196
9.3.2.	International terrorism.....	196
9.3.2.1.	Religiously motivated terrorism.....	196
9.3.2.2.	Non-Religious motivated terrorism.....	197
9.3.3.	Terrorist Financing threat assessment.....	197
9.3.3.1.	Domestic terrorism financing.....	197
9.3.3.2.	International terrorism financing.....	198
9.3.4.	Terrorism financing vulnerability assessment	198
ANNEXES	200
I. THREATS	200
II. NATIONAL VULNERABILITY	202
III FINANCIAL CRIMES INCESTIGATION AGENCIES	211
IV TYPES OF LEGAL DOCUMENTS	213
V CAPITAL MARKET SECTOR	218

Table of tables

Table1 – Overall money laundering risk in the jurisdiction.....	19
Table2 – Sectors: vulnerability – threat - risk.....	20
Table3- Crimes against property cases2014-2016	24
Table4- Organiced criminal groups 2014-2016	25
Table5-Frauds 2012-2016	26
Table 6- Seizures of cigarettes 2012-2016	27
Table7- Tax evasion amounts and verified tax and fines	30
Table8- Table of variables of national vulnerability for ML	38
Table9- Priority ranking for input variables.....	39
Table10- Overall national sectoral vulnerability	40
Table11-National vulnerability graphs	41

Table12- Vulnerability map	42
Table13- Total reported seizures.....	47
Table14- Frozen bank accounts.....	48
Table15- Capital market freezes.....	49
Table16- Suspicious transaction and information reports.....	51
Table17- ML Cases (originating from the above reports and information	52
Table18- Cases sent to the Public Prosecutor following freezing orders & corresponding criminal proceeds.....	52
Table19- Cases for investigation - action - information	52
Table 20 – Number of Judges and Prosecutors 2014-2016.....	55
Table 21- Controls performed in the year 2015	58
Table 22- Liquid asset controls 2014-2016.....	59
Table 23- Extraditions and European warrant arrests	62
Table 24- Judicial assistance requests (Prosecutor’s Office of Athens Court of Appeal)	62
Table 25- Information exchange requests through ARO-CARIN	64
Table 26- Special Secretariat of Financial and Economic Crime Unit (SDOE) Incoming information requests EUROPOL-INTERPOL	64
Table 27- Requests for exchange of information through FIU.net & Egmont Secure Web.....	64
Table 28- Administrative cooperation information exchange requests IAPR.....	65
Table 29- - Requests of exchange of assistance requests with EU Member States.....	66
Table 30- Requests of Exchange of Assistance Requests with third countries	66
Table 31- Statistics on the banking sector for the years 2012-2016.....	77
Table 32- Banking Sector: Assessment of general AML/CFT controls.....	80
Table 33- Banking Sector : Final product/service vulnerability.....	91
Table 34- Capital Market Sector: Investor participation in the total capitalization of ATHEX, 2016.....	100
Table 35- Capital Market Sector: ATHEX cumulative data, 2012-2016.....	102
Table 36- Capital Market Sector: Assets under management, 2016.....	102
Table37- Capital Market Sector: Assessment of general AML controls.....	103
Table 38- Capital Market Sector: Onsite audits.....	104
Table 39- Capital Market Sector: Corrective measures and Fines imposed, 2012-2016.....	105
Table 40- Capital Market Sector: STRs submitted to FIU, 2012-2016.....	106
Table 41-Capital Market Sector: Staff training during 2012-2016	106

Table 42- Capital Market Sector:Staff training during 2012-2016	107
Table 43- Capital Market Sector: Staff training during 2012-2016	107
Table 44- Capital market Sector: Inherent Vulnerability.....	108
Table 45- Life insurance Sector - Evaluation of general AML controls.....	111
Table 46- – Life insurance sector – Inherent vulnerability per life insurance product	119
Table 47– Life insurance sector – Product vulnerability (market share 2016)	119
Table 48- Life insurance sector – Inherent vulnerability level per product	121
Table 49- Other FIs: ML vulnerability	125
Table 50- Other FIs: Inherent ML vulnerability	126
Table 51- Other FIs: General AML controls	133
Table52- DNFBPssectors	141
Table53- Vulnerability assessment of DNFBPs sectors	142
Table54- DNFBPssectors: Assessment of input variables.....	144
Table 55- DNFBPs sector: Audits and violations in pawnshops	160
Table 56- DNFBPs sector: Violations of pawnbrokers for the years 2013-2017	161
Table 57- HAASOB – Quality controls 2012-2016.....	184
Table 58- HAASOB- Applications, approvals and rejections 2012-2016	185
Table 59- Revenues 2014-2016	188

Table of Figures

Figure1- National money laundering risk	17
Figure2- Assessment of national ML vulnerability	18
Figure3-Seized drug substances 2014-2016	22

Acronyms and Abbreviations

IAPR (ΑΑΔΕ)	Independent Authority of Public Revenue
HELLENIC POLICE HQ (ΑΕΑ)	Hellenic Police Headquarters
GDP	Gross Domestic Product
ARO-FECU	Asset Recovery Office- Financial Economic Crime Unit
FIU/Authority	FIU - Financial Intelligence Unit
ΑΥΣ	Suspicious Transactions Reports
GSPR	General Secretariat of Public Revenue
GDEP (ΓΔΟΠ)	General Directorate of Economic Policy
GSAC	General Secretariat Against Corruption
DMPR (ΔΔΔΥ)	Directorate for Management of Public Revenue
FCIS (Δ.Ε.Ο.Ε.)	Financial Crime Investigation Service
FPD (DOA)	Financial Police Division
DOY (Δ.Ο.Υ.)	Tax office
ISA	International Standards of Auditing
S.S./FECU (Ε.Γ. Σ.Δ.Ο.Ε)	Special Secretariat of Financial and Economic Crime Unit
HGC (Ε.Ε.Ε.Π)	Hellenic Gambling Commission
HAASOB	Hellenic Accounting and Auditing Standards Oversight Board
(IF) ΕΠΕΥ	Investment Firms
ENM	National School for the Magistracy
N.C.C.B.C.I.A	National Coordination Center For Border Control, Immigration and Asylum
N.Q.C.D. (Ε.Σ.ΠΑ)	National Quality Council for Development
E.D. (Ε.Φ.Κ.)	Excise duty
S.S.S.F. (ΕΦΚΑ)	Single Social Security Fund
(M.A.T.) Κ.Ο.Ε.	Mobile Audit Teams
T.P.C.	Tax Procedures Code
ITC	Income Tax Code
HCG	Hellenic Coast Guard
UN	United Nations Organization
OECD	Organization for Economic Co-operation and Development
NRA	National Risk Assessment

ML/TF	Money Laundering / Terrorism Financing
PEP	Politically Exposed Persons
O.C.C.A.S. (Σ.Ε.Κ.)	Operational coordination center against smuggling
(HLI) SEPE	Hellenic Labor Inspectorate
BAPAR (Σ.Μ.Τ.Λ. &Λ.Π.)	Bank Accounts and Payments Accounts Registry
CIACU (Σ.Ο.Ε.Ε.)	Central Inspection and Auditing Coordinative Unit
CADCU/NIU (ΣΟΔΝ/ΕΜΠ)	Central Anti-Drug Coordinative Unit/National Intelligence Unit
CoS (ΣτΕ)	The Council of State
CCMS (ΣΥΚΕΑΑΠ)	Coordination Center for Market Surveillance and the Fight against Illegal Commerce
MoF (ΥΠΟΙΚ)	Ministry of Finance
G.G	Official Government Gazette
VAT	Value Added Tax
FATF	Financial Action Task Force
ICPAG (SOEL)	Institute of Certified Public Accountants of Greece
HPCPM (GSEVEE)	Hellenic Confederation of Professionals, Craftsmen & Merchants
REFG (ΟΜΑΣΕ)	Real Estate Federation of Greece
CDD	Customer Due Diligence
CRD	Capital Requirements Directive
CRS	Common Reporting Standard
EBA	European Banking Authority
ESA	European Supervisory Authorities
Fintech	Financial Technology
HNWI	High Net Worth Individual
IT	Information Technology
KYC	Know Your Customer
L/C	Letter of Credit
L/G	Letter of Guaranty
MFI	Monetary Financial Institution
MOU	Memorandum Of Understanding

NPE	Non Performing Exposure
POS	Point of Sale
PSI	Private Sector Involvement
RBOAT	Risk Based Off sight Analytical Tool
Regtech	Regulatory Technology
SEPA	Single Euro Payments Area
SNRA	Supranational NRA
TBML	Trade Based Money Laundering
ED (ΑΔΣ)	Executive Director
GDP	Gross Domestic Product
STR (ΑΥΣ)	Suspicious Transaction Report
DD (ΔΕ)	Due Diligence
SIID (ΔΕΕΕ)	Supervised Institutions Inspection Department
IMF	International Monetary Fund
EU	European Union
ECB	European Central Bank
EEA	European Economic Area
PISC (ΕΠΕΙΑ)	Private Insurance Supervision Committee
HBI	Hellenic Banking Institute
HFSF	Hellenic Financial Stability Fund
LSI	Less Significant Institution
MFI	Monetary Financial Institution
PD	Presidential Decree
FI	Financial Institution
BoG	Bank of Greece
FO (ΧΟ)	Financial Organization

INTRODUCTION

This report serves as the first National Risk Assessment on money laundering and financing of terrorism that was drafted in Greece in accordance with Directive (EU) 2015/849 (4th EU directive)¹ and international standards.

The Committee for the Elaboration of a Strategy and Policies to deal with Money Laundering and Terrorist Financing (herein after referred to as “Strategy Committee”), as defined in Article 9 of Law no. 3691/2008, decided on the establishment of seven (7) working groups to assess the money laundering risk on a national and sector level and one (1) working group to assess the terrorist financing risk based on the World Bank’s ML/FT risk assessment methodology. In these groups participated, representatives of all the public authorities and bodies that are directly or indirectly involved in the prevention and suppression of money laundering and terrorist financing as well as representatives from the private sector and academic community.

In the following figure the methodology of the world bank for assessing the national and sector risk in relation to threat and vulnerability is illustrated.

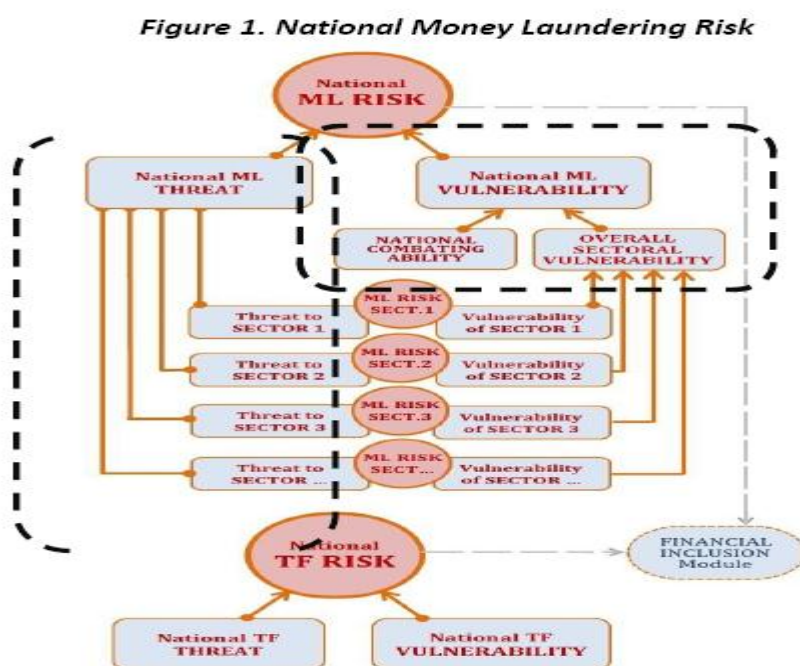


Figure1- National money laundering risk

In order to assess national vulnerability, the national ability to combat money laundering in combination with individual sectoral vulnerabilities was taken into consideration. The risk assessment group’s findings on terrorist financing are expressed in a separate confidential report and the summary constitutes an integral part of this report.

¹Articles 6,7 and 8 of Directive (EU) 2015/849

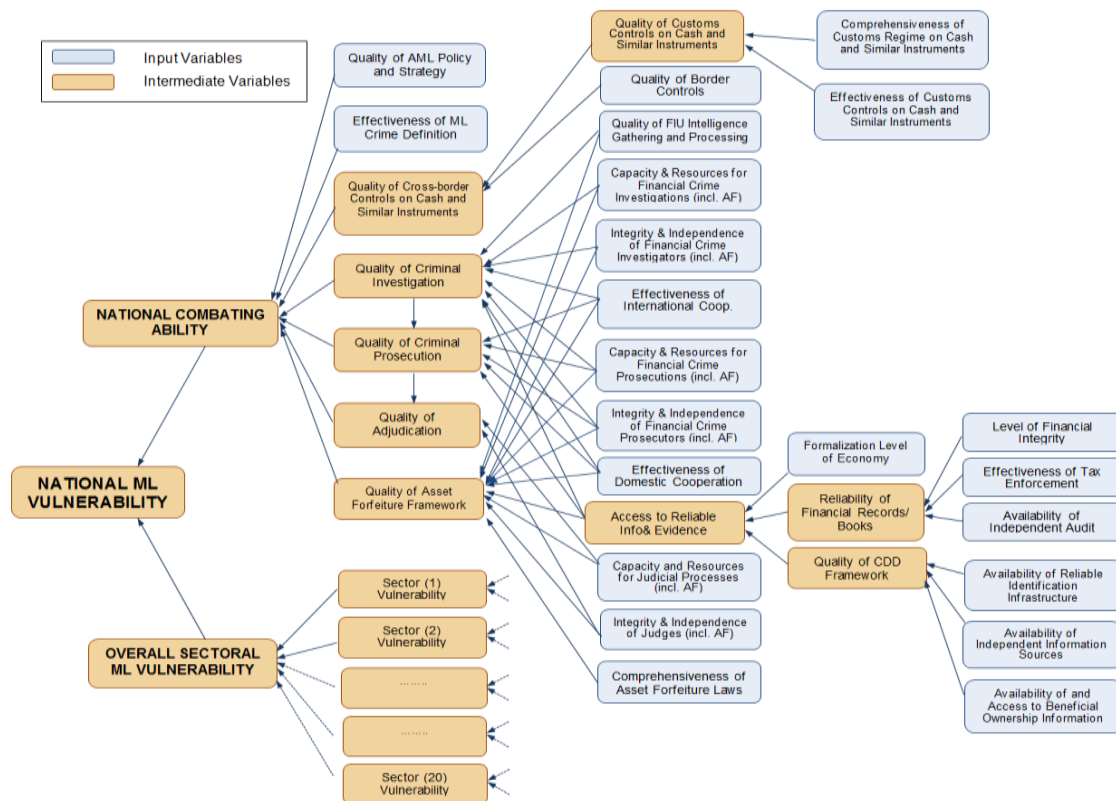


Figure2- Assessment of national ML vulnerability

The World Bank’s methodology points out the most significant threats and vulnerabilities in relation to money laundering in order to constitute the basis for the National Action Plan.

It should be pointed out that this Report refers to the national threats and vulnerabilities at the time of writing. Thus, it needs to be updated on a regular basis, at least biannually², and/or sooner in case of significant socio-economic changes.

As part of the preparation of the national ML/TF risk assessment, the competent groups reviewed quantitative and qualitative data that was made available to them by the relevant bodies and conducted interviews with experts on these issues. All the data was analysed in accordance with the methodology used by each group in order to evaluate the individual threat and vulnerability variables and finally to assess the overall ML/TF risk on a national level.

The National ML/TF Risk Assessment Report was approved by the Strategy Committee.

²Article 6 par. 7 of Directive (EU) 2015/849

1. RISK ASSESSMENT

1.1. Overall money laundering risk in the jurisdiction

According to the World Bank’s methodology, the national money laundering risk is assessed at “Medium High”. Taken into consideration, in order to assess the national risk, were the national threat level, which was assessed as “Medium High”, in combination with the national vulnerability level which was assessed as “Medium”. The following heatmap³ illustrates the national ML risk assessment that was adopted.

OVERALL MONEY LAUNDERING RISK IN THE JURISDICTION						
OVERALL THREAT	HIGH (H)	M	M	MH	H	H
	MEDIUM HIGH (MH)	M	M	MH	MH	H
	MEDIUM (M)	ML	M	M	MH	MH
	MEDIUM LOW (ML)	ML	ML	M	M	M
	LOW (L)	L	ML	ML	M	M
		LOW (L)	MEDIUM LOW (ML)	MEDIUM (M)	MEDIUM HIGH (MH)	HIGH (H)
OVERALL VULNERABILITY						

Table1 – Overall money laundering risk in the jurisdiction

1.2. Sector risks

With respect to the risks, assessed in the report is the threat for all the sectors that had been used to assess sectoral vulnerability. As shown, the highest risk level (HIGH) arises in the non-financial sectors (lawyers, notaries, accountants and real estate agents).

A “High” ML risk level is also observed in the money remittance providers sector followed by the banking sector which marks a “Medium High” risk level. The remaining sectors mark a lower risk level, as broken down in the following table.

³The 5x5 table assesses the risk level in relation to the threat and vulnerability in five (5) gradations, namely: LOW (L), MEDIUM-LOW (ML), MEDIUM (M), MEDIUM-HIGH (MH) and HIGH (H).

SECTORS	VULNERABILITY	THREAT	RISK
BANKS	MEDIUM	HIGH	MEDIUM HIGH
LIFE INSURANCE COMPANIES	MEDIUM LOW	MEDIUM LOW	MEDIUM LOW
LEASING COMPANIES	LOW	LOW	LOW
FACTORING COMPANIES	MEDIUM LOW	LOW	MEDIUM LOW
MONEY REMMITTERS	MEDIUM HIGH	HIGH	ΥΨΗΛΟΣ
E-MONEY INSTITUTIONS	MEDIUM	MEDIUM LOW	MEDIUM
BUREAUX DE CHANGE	MEDIUM	MEDIUM LOW	MEDIUM
INVESTMENT SERVICES COMPANIES	MEDIUM	MEDIUM LOW	MEDIUM
FUND AND ASSET MANAGEMENT COMPANIES	MEDIUM LOW	MEDIUM LOW	MEDIUM LOW
PORTFOLIO INVESTMENT COMPANIES	LOW	LOW	LOW
RECEIVAL AND TRANSMISSION OF ORDERS COMPANIES	LOW	LOW	LOW
LAND BASE GAMBLING SERVICES	MEDIUM HIGH	MEDIUM	MEDIUM HIGH
ONLINE GAMBLING SERVICES	MEDIUM	MEDIUM LOW	MEDIUM
ACCOUNTANTS	HIGH	HIGH	HIGH
AUDITORS	MEDIUM	MEDIUM	MEDIUM
NOTARIES	HIGH	MEDIUM HIGH	HIGH
REAL ESTATE AGENTS	MEDIUM HIGH	HIGH	HIGH
LAWYERS	HIGH	HIGH	HIGH
DEALERS IN HIGH VALUE GOODS	MEDIUM HIGH	MEDIUM	MEDIUM HIGH
PAWN BROKERS	MEDIUM HIGH	MEDIUM	MEDIUM HIGH

Table2 – Sectors: vulnerability – threat - risk

2. THREAT

2.1. Summary

The analysis aims to define the nature and type of criminal activity from which most proceeds originate as well as the greatest money laundering threat. In order to make this assessment, the report was based on quantitative and qualitative data⁴ from law enforcement authorities (Hellenic Police, Special Secretariat of Financial and Economic Crime Unit and Customs Authorities), supervisory authorities, the Authority and the Independent Authority for Public Revenue as well as qualitative data from prosecutorial and judicial authorities. It was also supported by data from research conducted by recognised institutions⁵ and reports by international organisations⁶.

From the analysis, the offenses with the highest ML threat level include:

- Drug Trafficking
- Corruption
- Crimes against property
- Financial Crimes
- Smuggling of Migrants and Refugees
- Tax offenses

Other offenses that do not pose a particular ML threat are not included in the analysis.

The threat for the banking and money remittance providers sectors have been assessed as “High”. Similarly, accountants, lawyers and real estate agents have also been assessed as “High”.

Greece does not constitute a money laundering safe haven⁷. The years 2014-2016 marked a boost in the real estate market by foreign nationals⁸ and companies, part of which may constitute high risk transactions.

The national threat level is assessed as “Medium High”.

⁴Statistical data, open sources, qualitative features of cases and assessments by experts in the public and private sector.

⁵Final reference of the “Organised Crime Portfolio”, which includes the level of illicit proceeds for 7 EU countries, Greece being among these.

⁶E.C., Europol, Interpol, FRONTEX, GRECO, etc.

⁷“Organised Crime Portfolio”, 2015

⁸Law no. 4146/2013(Government Gazette A 90/18-04-2013) “Creation of a Development-Friendly Environment for Strategic and Private Investments and other provisions”

2.2. Threat from predicate offenses

2.2.1. Drug Trafficking

Drug trafficking is the largest illegal market in Europe. More than 1/3 of active European criminal organisations are involved in the manufacture, trade and trafficking of the narcotic substances, generating proceeds of at least 24 billion Euro per annum.⁹

Greece acts as a narcotics “gateway” in the EU. Its unique geomorphological characteristics and extensive coastline, its countless islands and strategic positioning between three continents make it an area of activity for international drug trafficking networks. It is situated on the “Balkan Axis”, one of the main drug trafficking “routes”, which unites the world’s largest opium production countries (Afghanistan, Iran, Pakistan, Myanmar, Laos) with the respective north-western European countries that consume these manufactured narcotics.

Moreover, it acts as a transit point for organised crime groups for cannabis and heroin, from Albania and Turkey, respectively, as well as significant hauls of cocaine from Latin American countries. According to available data¹⁰, the jurisdiction of origin of the drugs confiscated in Greece in 2014-2016 are depicted below:

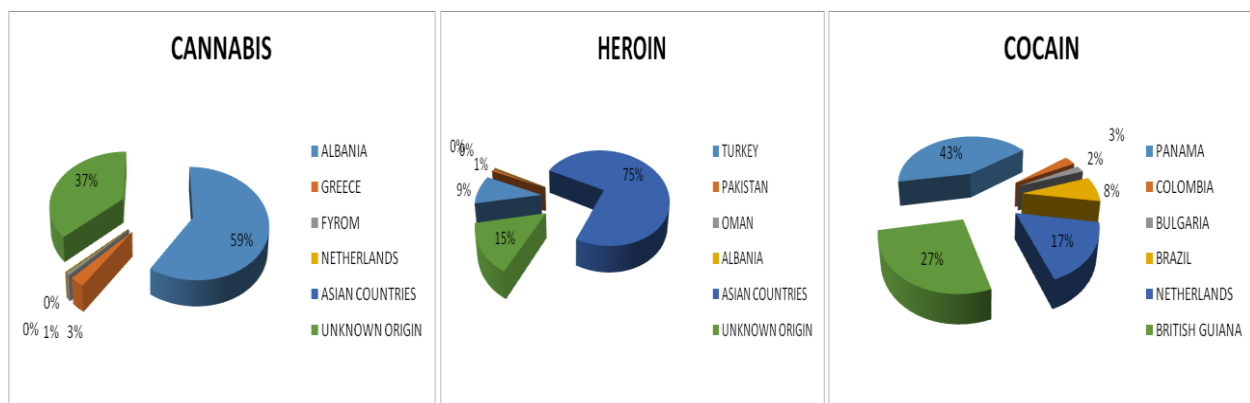


Figure3-Seized drug substances 2014-2016

The drug trade is one of the most lucrative illicit activities with estimated “proceeds” in the years 2014, 2015 and 2016¹¹ of €188,000,000, €62,000,000 and €200,000,000, respectively¹². In these years, the trafficking of cocaine, heroin and cannabis in Greece by organised crime groups reaches 75%, 83%, and 35% respectively. A total of 188 criminal organisations, whose members consisted primarily of Greeks and Albanians followed by Bulgarians and Nigerians, were dismantled¹³.

The drug trade is primarily cash based, which makes it difficult for law enforcement authorities to identify illicit proceeds.

⁹ Serious Organised Crime Threat Assessment, SOCTA,2017 https://www.europol.europa.eu/sites/.../socta2017_0.pdf

¹⁰ Reports of serious organised crime in Greece in 2014-2016, Central Anti-drug Coordination Unit Reports. 2014-2016

¹¹ Internal Confidential document, Hellenic Police Headquarters/Directorate of Public Security.

¹² gross profit from the total quantities of drugs that were confiscated based on indicative trafficking prices

¹³ Report on Serious Organised Crime 2014 (p. 30), 2015 (p.46), 2016 (p. 43)

Money laundering resulting from drug trafficking is primarily executed via legal cash-intensive business structures (e.g. restaurants, recreational businesses), the real estate or high-value goods market, the use of winning land-based betting tickets and the transfer of funds to off-shore companies.¹⁴⁻¹⁵

2.2.2. Corruption

The assessment of corruption in Greece presents a multitude of difficulties, firstly due to the lack of a fixed methodology for assessing the phenomenon, secondly due to the broad sense of the definition and the large number of cases that are not reported and officially recorded, resulting in insufficient data.

According to the recent report by “Transparency International”, the global, non-governmental organisation, which constitutes the most widely-used corruption indicator worldwide (corruption perception index), out of a total of 180 countries Greece ranks 59th in 2017¹⁶ from 69th in 2016.

In order to assess the corruption threat level, consideration has been given to crimes of bribery¹⁷, misappropriation¹⁸, the abuse of functions and embezzlement²⁰, according to the United Nations Convention against Corruption²¹.

Based on the report²² by the General Secretariat for the Fight against Corruption (GSAC)²³ criminal misappropriation of public funds presents the highest criminal prosecution rates²⁴. Significant cases relating to corruption by civil servants over the last 10-15 years have been investigated including *Politically Exposed Persons* (PEPs), which have been referred to the Greek judicial authorities.

Money laundering in serious cases of corruption is mainly effected via accounts held at foreign banks that maintain the strictest bank secrecy laws, via international credit centres in the name of offshore companies and investments in the real estate market.²⁵

The following two cases are given as examples:

- the case of a former minister who requested and received 55 million Euro during the award and materialisation of arms programmes. The funds were channelled via an intertwined network of domestic legal persons or offshore companies, a large number of associates that appeared as true beneficiaries and an extensive number of bank transactions via domestic and foreign banking institutions aimed at the transfer, concealment and laundering of part of these funds via domestic investments (mainly domestic property).

¹⁴Report on Serious Organised Crime 2016 of the Hellenic Police, p. 48
<http://www.astynomia.gr/images/stories/2017/files17/07112017ethsiaekthesi2016.pdf>

¹⁵ Qualitative analysis of Hellenic Police Headquarters cases,

¹⁶https://www.transparency.org/news/feature/corruption_perceptions_index_2017

¹⁷ Bribery consists of the offering or giving to public or political officials, judges, civil servants or other government officials, as well as foreign public officials and officials of international organisations.

¹⁸Articles 256 and 390 Penal Code

¹⁹ Misappropriation, with respect to the public service, constitutes a felony in three circumstances (provided that certain individual circumstances apply): a) if the offender uses special deception techniques and the reduction of the property is of a particularly high value, a maximum total of 30 thousand Euro, or b) if the object of the offense is greater than 120 thousand Euro, or c) if the loss that was caused or was threatened is greater than 150 thousand Euro.

²⁰Art. 258 in combination with Art. 375 Penal Code

²¹ Ratified with Law no.3666/2008 - Government Gazette 113/A/18.6.2008. The offenses referred to in this report correspond to Articles 15 to 17 of the United Nations Convention against Corruption.

²² Corruption Data Collection Report, p. 10,
<http://www.gsac.gov.gr/attachments/article/142/%CE%91%CE%A0%CE%95%CE%99%CE%9A%CE%9F%CE%9D%CE%99%CE%A3%CE%97%20%CE%A3%CE%A5%CE%9B%CE%9B%CE%9F%CE%93%CE%97%CE%A3%20%CE%94%CE%95%CE%94%CE%9F%CE%9C%CE%95%CE%9D%CE%A9%CE%9D%20%CE%94%CE%99%CE%91%CE%A6%CE%98%CE%9F%CE%A1%CE%91%CE%A3.pdf>

²³The GSAC was founded with Law no. 4320/2015 as an institutional, coordinating body with powers to supervise, audit, define priorities and take initiatives at political and legislative level for all anti-corruption control mechanisms, structures and services.

²⁴ See. Annex

²⁵ Data from the qualitative analysis of cases

- indicative case of fraud in which the owners of private energy companies embezzled 254.5 million Euro that ought to have been attributed to the Greek State. In order to conceal these funds they used Greek and foreign banks as well as an extensive network of offshore companies. As a result the threat level is significantly higher in the case of major fraud (especially against the Public service and significant legal persons or credit institutions).

It is considered that the real estate sector has also been used in a large number of money laundering cases that are linked to corruption, mainly due to the concealment of the actual value during the sale of the property and the presentation of values that are much lower than the market values. It should be noted, however, that the inherent risk in the real estate market has been significantly mitigated (great reduction in transactions, convergence of market and objective values).

The domestic banking sector has also been used in the laundering of cases that are linked to petty crimes of corruption, mainly via the complicity of funds that originate from both illegal and legal sources. Lastly, the use of medium-term investment products in combination with life insurance policies has been observed abroad as a means of channelling bribe proceeds to other financial products.²⁶ This is an attractive vehicle because the illicit proceeds are transferred closer to the main crime's statute of limitation period.²⁷

2.2.3. Crimes against property

As presented in the table below, the rate of property crime cases, specifically robberies and thefts, are particularly high in relation to the public-order crimes committed²⁸.

Cases per year, as a percentage of the total public security crimes	2014	2015	2016
Robberies	3,05%	3,36%	3,58%
Thefts (except vehicle thefts)	55,51%	57,18%	56,98%
Vehicle thefts	19,48%	19,66%	19,03%
Total (property crimes)	78,04%	80,21%	79,59%

Table3- Crimes against property cases 2014-2016

It is difficult to accurately estimate illicit proceeds that are linked to the above crimes. The loss that is caused by criminal organisation is greater when compared to the loss that is caused by individual, small-scale perpetrators, since they act as an organised, massive-scale with greater technical specialisation, aiming at higher profits. The perpetrators' goal plays an important role with regard to the size of the proceeds.

Based on the number of detected cases concerning organised criminal groups in 2014-2016, the following data arises²⁹:

²⁶ Athens Appeals Court Decision No. 2973/2017.

²⁷ Data from the qualitative analysis of cases

²⁸ Statistical Data-Directorate of Public Security/Hellenic Police Headquarters.

Criminal organizations/groups per year	2014	2015	2016
Criminal organizations/groups involved in property crimes	163	151	163
Criminal organizations /groups involved in property crimes, as a percentage of the totally investigated criminal organizations	54,1%	42,41%	45,53%
Estimated proceeds of the investigated criminal organizations/groups	11 million €	11,5 million €	57,7 million €

Table4- Organiced criminal groups 2014-2016

Analysis of the Hellenic Police’s data indicate, that in their majority criminal organisations do not have interconnections with international criminal groups. The groups that engage in thefts (excl. vehicles) and robberies consist mainly of Greek, Albanians and Georgians.³⁰

The theft of vehicles and their trade is mainly controlled by combined, international criminal groups, whose members primarily originate from Eastern European countries. These criminal groups use Greece as the jurisdiction of origin, destination and transit of the stolen vehicles or their spare parts. The laundering of these proceeds is done via companies or legal formations that specialise in the purchase and repair of vehicles.³¹

From the qualitative analysis of the Hellenic Police’s data, it arises that the proceeds that arise from property crimes are primarily used to purchase high-value goods (luxurious vehicles and jewellery), while a portion of these proceeds is also invested in the real estate market. Moreover, it is also noted that some of the stolen goods are pawned in order to be converted into cash. Lastly, when the proceeds from the above crimes are sent out of the jurisdiction, the physical transportation of cash (cash couriers) and the use of money remittance providers is observed.

2.2.4. Financial crimes

Of all the financial crimes³² those that present the highest threat risk were selected, namely the crimes of fraud³³ (including internet fraud³⁴) and forgery³⁵, while the crimes of smuggling³⁶ and the black market were included for reasons of coherence.

Fraud has always constituted a significant and profitable criminal activity both for the jurisdiction’s sole perpetrators and organised criminal groups. The following Table³⁷illustrates the overall extent of this criminal activity³⁸:

²⁹Report on Serious Organised Crime 2014 (p. 34),2015 (p.49) ,2016 (p. 50) by the Hellenic Police

³⁰Report on Serious Organised Crime 2014 (p. 37),2015 (p.52), 2016 (p.54) by the Hellenic Police

³¹Report on Serious Organised Crime 2014 (p. 38), 2015 (p. 53), 2016 (p. 55) of the Hellenic Police

³² Articles 385-406 Penal Code

³³Article 386 Penal Code

³⁴Article 386A Penal Code

³⁵Article 216 Penal Code

³⁶Articles 155, 156 and 157 of Law No. 2960/2001 (A 265)

³⁷ Data from the Hellenic Police Headquarters

³⁸The rising trend appearing in 2016 (4,979 cases of fraud compared to 3,596 in 2015, namely an increase of 38.46%), is due to the large number of recorded fraud attempts (1,189 attempts in 2016 compared to 428 in 2015), which primarily concerned attempts of defrauding

FRAUDS							
	COMMITTED	ATTEMPTED	TOTAL	INVESTIGATED	NATIVES	ALIENS	TOTAL
2012	3.166	163	3.329	1.283	1.070	113	1.183
2013	2.860	165	3.025	1.359	1.004	149	1.153
2014	2.877	158	3.035	1.426	1.087	144	1.231
2015	3.168	428	3.596	1.515	954	235	1.189
2016	3.790	1.189	4.979	2.066	992	247	1.239

Table5-Frauds 2012-2016

The overall profit that was reaped by the criminal groups that were detected in 2015 and 2016 by the Hellenic Police is estimated at €3,600,000 and €2,630,000, respectively.³⁹

The majority of frauds are committed by individuals, they target vulnerable victims (e.g. the elderly, people that purchase products and goods online) and the proceeds from these is much lower when compared to cases where the victims are public sector agencies and/or companies.

The organised groups are equipped with equipment for the falsification of documents and/or collaborate with counterfeiters as well as other professional groups (doctors, lawyers, notaries, etc) to facilitate their criminal activities. The activities of such groups are multifaceted.

“Internal” fraud at the expense of credit institutions, where the proceeds may be high, is a specific case. The main source of the ML risk originates from frauds that are committed by borrowers and low or, on occasion, high-ranking bank officers via the circumvention of loan granting procedures. If committed, they present inherent advantages in terms of money laundering, but also in the concealment and transfer of the loan’s amount to other Banks in Greece or abroad or its withdrawal in cash. Adversely, the phenomenon of internal fraud that relates to the misappropriation of customers’ bank accounts, is mainly combined with crimes of forgery and defrauding and presents an increased degree of difficulty in the concealment and laundering of the proceeds. In the past, it primarily concerned low-ranking employees of managers at individual branches that sought to take advantage of the funds quickly (via gambling, investments) so that they are returned to the beneficiary without being noticed.

However, the above forms of fraud are committed in a very different economic environment and internal controls’ environment of credit institutions. The significant reinforcement of the Credit Institutions’ internal controls systems in recent years has mitigated the banking sector’s exposure to such fraud.⁴⁰

the elderly over the phone, using the pretence of an accident, Report on Serious Organised Crime 2014 (p. 49), 2015 (p. 75), 2016 (p. 78) of the Hellenic Police

³⁹Report on Serious Organised Crime 2015 (p. 75), 2016 (p. 79) of the Hellenic Police

As it arises from an indicative case of misappropriation and fraud, the CEO, the primary shareholder and other members of a bank’s Board of Directors approved large loans to natural or legal persons. The economic profile of these persons could not justify the loan amount, whereas the collaterals provided to the bank were insufficient. In this case, the bank was placed under special liquidation.

It should be noted that internet fraud has marked an increase in recent years, even though the proceeds from this criminal activity are currently low⁴¹.

With respect to forgery, it appears as a secondary crime in confluence with other forms of criminal activity and is directly correlated with transactions of a financial and administrative nature, significantly affecting their smooth processing. It is for this reason that it is considered to be of little importance and an independent criminal activity in relation to other financial crimes and laundering.

Furthermore, smuggling is a significant and lucrative activity for criminal groups. The main forms of this criminal activity is the smuggling of tobacco products, alcohol and fuel. It should be noted that tobacco products, fuel and alcohol are subject to specific excise tax.

According to available data, tobacco products and particularly cigarettes⁴², have steadily constituted the majority of all products that are smuggled in recent years. Consequently, the smuggling of tobacco products constitutes the greatest threat of the money laundering sector. The key incentive for this illicit activity is the high taxes on the tobacco products⁴³, which in recent years has become disproportionate with the consumers’ buying power, thus boosting the consumption of smuggled products.

From 2012 to 2016, the Greek law enforcement authorities have carried out 10,304 seizures with 2,546,033,977 cigarettes being confiscated. The relevant table follows⁴⁴:

SEIZURES OF CIGARETTES						
YEAR	2012	2013	2014	2015	2016	ΣΥΝΟΛΟ
QUANTITY (in pieces)	468.575.08	467.293.37	428.802.919	634.972.879	546.389.730	2.546.033.977
ESTIMATED DUTIES AND TAXES (in €)	71.138.04	71.926.89	75.741.023	115.281.813	97.749.986	431.837.755
SEIZURES	1.234	1.756	2.245	2.659	2.410	10.304

Table 6- Seizures of cigarettes 2012-2016

⁴⁰The reasons are thoroughly analysed in the respective Sectoral Vulnerability chapters (Staff Integrity, Criminal Sanctions, Vulnerability of loan products), noting the decreasing trend in the number of serious operational risk cases.

⁴¹ In 2013-2016, 225 cases were detected by the Hellenic Police Headquarters Financial Police & Cyber Crime Agency. Of these, 139 were “business e-mail compromise” (or Man-in-the-Middle) cases with proceeds of approximately € 10,000,000, and 75 were “money muling” cases with estimated illicit proceeds amounting to € 500,000. (Internal Confidential document, Financial Police & Cyber Crime Agency)

⁴² It should be noted that in Greece, at an estimated rate of 85%, cigarettes constitute the highest revenue due to the Excise Tax on tobacco products. Report on Serious Organised Crime 2016 (p. 61)

⁴³European Commission Excise Duty Tables. In 2016, Greece held third place in terms of the total tax charges (Excise Tax and VAT) on cigarettes bordering on 84%, https://ec.europa.eu/taxation_customs/sites/taxation/files/docs/body/excise_duties-part_iii_tobacco_en.pdf

⁴⁴ Data by the General Directorate of Customs and Excise Duty of the Independent Authority for Public Revenue (IAPR).

Taking into account Greece's geographical position and the energy products' VAT and Special Excise Tax rate on customs revenue (approximately 48% for 2016)⁴⁵, the smuggling of fuel constitutes a significant threat. According to the IAPR's data on seizures/freezing for 2016-2017, an increase of 607.7% is observed in oil products. Specifically, 313,254 litres of liquid fuel were confiscated in 2017.⁴⁶

The black market is defined as any movement, sale of merchandise in any way without the anticipated professional licence or the statutory receipts/invoices.⁴⁷ The black market falls within a broader circle of misconduct and at times coexists with other illicit activities, such as: concealment of taxable products, smuggling, infringement of intellectual property and trademark (imitation, falsification, pirating).

With regard to the marketing of imitation products, which primarily originate from China, Hong Kong and Turkey, it arises that Greece is a gateway for such products to the EU⁴⁸. Based on statistical data on the confiscation by the Hellenic Police⁴⁹ and the Special Secretariat of the Criminal Investigative Body (SDOE), these primarily concern the imitation of brand named products such as clothing, watches, bags and tech products. From the assessment of these data, it is ascertained that this criminal activity constitutes a significant threat for Greece.

2.2.5. Smuggling of migrants and refugees

Due to its geographical position, Greece constitutes a gateway to the EU for a large number of illegal economic migrants and refugees⁵⁰. The final destination for the majority these individuals are Central and Northern European countries. In 2015, Greece was forced to deal with an influx of refugees and migrants⁵¹ primarily due to the civil war in Syria. The illicit smuggling of migrants is conducted via an illegal network of smugglers that conduct their business outside the jurisdiction's borders. On a European level, the smugglers' revenue ranged between 4.7 and 5.7 billion⁵² Euro in 2015 and 2 billion Euro in 2016. With respect to the entry migrants into Greece, as is the case throughout the EU, the greatest part of the criminal groups' proceeds was received prior to their entry into the jurisdiction.⁵³

Moreover, facilitation of the illegal departure from the jurisdiction is a criminal activity and constitutes a significant money laundering threat given that it is very lucrative. Based on data provided by the Hellenic Police Headquarters, such proceeds were estimated at about €307,000,000 for 2015 and €367,000,000 for 2016⁵⁴. The vast majority of smugglers that were arrested, 88% in 2015 and 78% in 2016, are third country nationals that live in Greece illegally. It is worth noting that 1501 and 950 smugglers were arrested in 2015 and 2016, respectively.⁵⁵

The illegal smuggling networks collaborate with "workshops" that specialise in the preparation of high quality fraudulent travel and other documents with which they equip the illegal migrants and refugees.

⁴⁵General Secretariat of Public Revenue (GSPR) Report. 2016

⁴⁶IAPR Report. 2017,

⁴⁷Law no. 4155/13, Article 39 and 40

⁴⁸OECD EUIPO "Trade in Counterfeit and Pirated Goods (2016)"

⁴⁹Report on Serious Organised Crime in Greece 2015 (p. 64) and 2016 (p. 63), Hellenic Police

⁵⁰According to data provided by law enforcement authorities (Police, Port Authorities), the influx of migrants into Greece in the years 2012, 2013 and 2014, was 34,084, 12,556 and 45,421, respectively, namely 92,061 in total.

⁵¹From 2015 until early 2017, a total of 1,141,275 illegal migrants have been recorded. Of these migrants, 52,401 were repatriated, relocated according to the current International Treaties, 63,494 currently remain at Reception and Identification Centres, within and outside of other structures. The above data reveals that approximately 1,025,380 or 89.8% of these migrants have illegally departed from Greece to other member states under the Schengen Agreement, or remain in Greece with the majority waiting to depart illegally.

⁵²Europol Report, SOCTA

⁵³Data based on interviews with migrants at the reception/identification centres

⁵⁴Internal confidential document - Centre for Security Studies (KEMEA)

⁵⁵See. Annex

The majority of refugees and migrants receive remittances from their countries of origin via money remittance providers during their stay in Greece.

The smugglers do not carry out transactions via the banking sector, they do not engage with legal entities nor do they purchase property and/or luxurious items in order to launder their money. They usually use small businesses (trading in items of convenience, electronics and mobile phones) as front for the collection and distribution of funds. Members of the criminal groups are paid via money remittance providers and/or the unofficial payment network “Hawala” which operates within mini markets, mobile phone and/or electronic device stores, travel agencies owned by members of the groups.⁵⁶

An indicative case refers to a criminal group that illegally smuggled migrants from Greece to other European countries. Its members received up to 16,000 Euro per person, an amount that was illegally transferred via “HAWALA”, the unofficial money transfer system. According to the investigation, this criminal group facilitated in 26 illegal migrant departure cases from the jurisdiction.⁵⁷

In recent years, a number of NGOs have become active in Greece in relation to illegal migration. With respect to the NGOs in question, and all NGOs for that matter, a detailed provision is in place in article 10 of Law no. 3691/2008, which foresees the issuance of Joint Ministerial Decisions by the Minister of Finance and the competent Ministers on issues relating to companies, organisations, unions and other associations of persons of a non-profit nature, in order for necessary measures to be established for the prevention of this sector to be used for ML.

These measures include the keeping of a register of the above entities by a competent authority, per category, the mandatory processing of their main transactions via credit institutions and the conduct of sample audits by the competent public authorities, depending on the degree of risk. To date, individual registries of non-profit entities are kept at the competent Ministries, thus making it impossible to form a single, joint register.

2.2.6. Tax evasion – Tax offences

The term “tax evasion” encompasses offenses that are described in Article 66 of Law no. 4174/2013, as in force. Tax evasion is a predicate offense of ML and whoever commits tax evasion offenses is punished with at least 2 years imprisonment⁵⁸. It should be noted that non-payment of debts exceeding € 200,000 to the State is defined as a predicate offense based on Law no. 3691/2008, but is not included in the analysis that follows. Moreover, cases concerning non-criminal offenses or offenses that can be resolved via out-of-court settlement are not included.

According to the statistical data by the competent tax authorities for the years 2013 to 2016, the threat level for tax evasion was assessed to be High.

A table is provided below with the overall amounts corresponding to reports of tax evasion offenses to the Authority by the IAPR for the years 2013-2016 and the overall amount of verified taxes and fines that arose following tax audits.

⁵⁶Report on Serious Organised Crime 2016 of the Hellenic Police, p. 31

⁵⁷ The operation was jointly carried out by the Hellenic Police, Europol and the UK’s National Crime Agency following several months of investigation. See. relevant Europol website <https://www.europol.europa.eu/newsroom/news/migrant-smuggling-organised-crime-group-dismantled-in-greece>

⁵⁸ if taxes for undeclared income or assets exceeding the amount of € 100,000 per year and per tax type, or the value added tax of undeclared income resulting from sales, etc., exceed the amount of € 50,000 per year, or if any other illegal tax, tariff or contribution exceeds € 100,000.

	2013	2014	2015	2016
Tax evasion rates attributable to the number of reports of certified tax evasion over € 50,000 to the Authority under Law 3691/2008 (€ million)	112,40	137,90	896,91	631,75
Total veified taxes and fines from checks completed and some (€ million)	1.615,30	3.635,36	5.028,24	3.014,95

Table7- Tax evasion amounts and verified tax and fines

In the banking sector⁵⁹ the above threat assessment is considered high, since the majority of reports concerning suspicious transactions that are submitted to the Authority by the CIs concern transactions that may be related or linked with the tax evasion offense, however, with their quantity being reduced.

In addition, the non-financial sector encounters a high threat level since accountants, tax consultants, lawyers, notaries and real estate agents may act as tax evasion facilitators, especially with transactions that are associated with the buying and selling of property⁶⁰.

2.3. External threat level

In order to assess the jurisdiction's threat level from abroad pursuant to the World Bank's methodology, an analysis was conducted on the annual data of cross-border fund transfers that were carried out via the financial system during 2012-2016.⁶¹

Coming under review were the Balance of Payments statistical data held by the Bank of Greece and concern capital inflows to Greece per country of origin with respect to: payments for exported goods, provision of services, direct investments in the jurisdiction (establishment or business acquisitions, etc) purchase of share and bond portfolios and remittances. Also coming under review were capital outflows to foreign jurisdictions that concern reverse transactions (payments for foreign imports, direct investments to other countries, etc.). The study was focused on south-eastern European countries, high-risk countries, the 10 largest trading partners and countries/jurisdictions that do not comply for tax information exchange purposes.

The analysis of capital flows in comparison with those expected based on trade relations, etc., did not reveal any inconsistencies, thus no indications of inherent risk arose, mainly regarding the use of the banking sector, which compiles the majority of these transactions.

Data obtained from law enforcement, judicial and public prosecuting authorities reveals the participation of a large number of foreign nationals in criminal activities, a fact that increases the risk of these criminal proceeds being transferred to their country of origin.

The physical transfer of cash outside Greece cannot not be verified by the Customs Authoritie's corresponding data on cash movements. Moreover form the same data derives that also the incoming cash movements are relatively low.

⁵⁹ See. Analysis of Banking Sector Threat

⁶⁰Qualitative analysis of cases by the Authority of Article 7, Law no. 3691/08, IAPR, SDOE, Hellenic Police

⁶¹Bank of Greece data (Confidential File)

Furthermore, as it arises from the data by the National Asset Recovery Office, during the years 2013 - 2016, Cyprus had the most outgoing requests at a rate of 22.3%, followed by the UK and Bulgaria at rates of 10.5% and 8%, respectively. With respect to incoming requests, most came from the UK at a rate of 15.2%, followed by Germany, Bulgaria and Belgium at rates of 10.4%, 8.3% and 7%, respectively.

2.4. Threat level per sector

Data obtained from law enforcement, judicial and public prosecuting authorities and the self-assessment by the principal parties in terms of the money laundering threat gives rise to the following per sector:

2.4.1. Banking Sector

Traditionally, the banking sector encounters a significant ML threat primarily from tax evasion, fraud and corruption, due to its importance for the domestic economic activity in relation to the acceptance of deposits, the issuance of loans, the conduct or acceptance of payment transactions and the diversity and specialisation of financial services that it offers. In particular, the use of the banking sector was verified in various significant financial crimes that were committed in the past (up until 2009) and were either finally adjudicated by the legal system or their judicial inquiry commenced during the 2012-2016 five-year period. Moreover, it should be noted that on a financial sector level, the banking sector constitutes the main source of suspicious transaction reports submitted to the FIU, the majority of which possibly concern tax evasion. Nevertheless, via the specific reports that relate to inconsistencies between the amount being deposited to the customers' accounts and their economic profile, it is also possible to detect ML cases that are linked to predicate offenses.

It is worth noting that the attraction of the banking sector for ML purposes has been mitigated in recent years (e.g. reduction of suspicious transaction reports by -41% and cash transactions at credit institutions by -80% since 2012), a fact that is attributed to:

- the imposition of capital controls and restrictions on foreign fund transfers in 2015,
- the tax authorities' development of powerful tools since 2011 for the detection of tax evasion via the banking system. These tools include both regular reports for customers' transactions that are submitted to the authorities by the CIs and, vice versa, systems for authorities to access bank accounts following requests made by the Tax Offices and other Tax audit services (access to bank account register).
- the effective use of the above tools, as suggested by the rising number of verified additional taxes since 2012 as well as the large number of seizures/freezing that have been imposed.

The above, in combination with the reinforcement of the general ML/TF control and prevention mechanisms (e.g. addition of provisions to the regulatory framework regarding tax evasion since 2012, supervisory, organisational and computerised synergies due to the merger of the sector, etc.) have made it more difficult or have increased the possibility of detecting bank transactions that aim at laundering or concealing illicit funds (e.g. via remittance to foreign banks, or their withdrawal in cash).

To this end, although the Banking sector threat level is diminishing, it is assessed as "High".

2.4.2. Life Insurance Company Sector

As highlighted in the European Commission's report on the supra-national assessment of ML and TF risks at EU level, the use of life insurance products as a conduit for money laundering requires complex planning and knowledge in order to establish it a viable choice. The products that are offered by life

insurance companies in Greece are not as diverse or flexible in order to attract individuals that wish to launder illicit funds. Investment products are the type of insurance products that are usually included in the typologies of unusual or suspicious transactions for ML purposes. However, according to data for 2016, the annual amount from investment product premiums in Greece represents a mere 13% of the overall revenue from life insurance premiums (€ 1.9 billion, namely about 1% of the GDP). It should also be noted that in their majority, life insurance companies maintain long-term relationships with their clients due to the nature of the products, whereas occasional clients and transactions that entail a higher ML risk do not exist.

The insurance sector threat level arose from the offense breakdown within the various sectors, the ML threat realisation methods and the investment and laundering methods that arise from the conduct of the predicate offenses. Of the cases analysed, the life insurance sector did not demonstrate any involvement in money laundering activities. As a result, the ML threat level for the insurance sector was assessed as “Medium Low”.

2.4.3. Capital market sector

With respect to the money laundering threat, the capital market is not the sector of choice for criminal groups. The main reason being the low turnover (compared to the past) on the Athens Stock Exchange, the small value of managed funds, the increased complexity and the imposition of capital controls since June 2015. In spite of the above, the securities market may be used by criminals that are in search of complex systems to launder their proceeds. Money laundering cases that were conducted abroad have not been noted.

The capital market sector is broken down into the following four categories:

- a) Investment Services Companies (EPEY): the assets managed by the EPEY amount to 6% of the GDP and their products have medium to high complexity. The client’s funds are primarily directed to the EPEY via the banking system and in recent years there have not been any noteworthy ML/TF cases. The ML/TF threat, according to the report on the supra-national risk assessment, is graded as moderately significant, namely “medium-low”.
- b) Funds and Asset Management Companies. The report on the supra-national risk assessment deems the ML threat as moderately significant. In Greece, funds that are managed by these companies are relatively low, they concern long-term investments and are only accepted via the banking system, thus the threat is graded as “medium-low”.
- c) Companies that undertake the reception and transmission of orders do not accept funds, thus the complexity is very low and the threat is graded as “Low”.
- d) Portfolio Investment Companies are closed-end funds and encounter the same threat as any other listed company, thus the threat is graded as “Low”.

In the past, the capital market sector was used as a conduit for raising criminal proceeds via price fixing, especially between 1998 and 2002. In the period from 1998 to 2005, the Hellenic Capital Market Commission imposed administrative sanctions amounting to approximately 39 million Euro to 511 cases, whereas from 2006 until mid 2017 it imposed sanctions amounting to approximately 6 million Euro to 139 cases.

To this end, the threat level for this sector is assessed as “Medium Low”.

2.4.4. Other financial institutions

2.4.4.1. Money remittance providers

The geographical extent in which they provide their services, the use of cash and the occasional nature of the transactions make this an attractive sector for ML purposes, while the threat level for this sector further increases due to the extensive use of agents, most of which do not come from the financial sector (e.g. mini market owners). In addition, it has been verified that this sector has transaction motifs that fall under the typology of suspicious transactions.

According to the FATF report: “Money Laundering through Money Remittance and Currency Exchange Providers”, money remittance providers are regularly used as a vehicle for laundering illicit proceeds relating to the following crimes: drug trafficking, fraud, economic crimes, trafficking in human beings, theft and smuggling. According to the European Commission’s Supra-National Risk Assessment, money remittance providers are used by criminals primarily because the remittance services are easily accessible and do not require particular knowledge or techniques for laundering proceeds.

Based on the offense breakdown, the main ML threats for the money remittance providers’ sector concerns illicit proceeds from:

- 1) Illegal migration and accompanying offenses including the falsification of travel documents
- 2) Thefts, robberies and other property crimes

It should be noted that the capital controls that were imposed in July 2015 and especially the controls that were imposed on the transmission of remittances abroad both at customer and money remittance provider level, reduced the attractiveness of this sector for ML purposes

Nevertheless, the threat level for the money remittance providers sector is “High”.

2.4.4.2. E-money issuers

According to the European Commission’s Supra-National Risk Assessment, e-money is attractive for criminal organisations. The Financial Information Units (FIUs) in the European Union have detected numerous cases of tax fraud, drug trafficking and prostitution via the purchase of numerous prepaid payment cards.

The remote execution of transactions constitutes a feature of e-money issuers, which increases their attractiveness for laundering purposes.

That said, the quantity of e-money issued in Greece is low. Moreover, capital controls that were imposed in July 2015 have made this sector less attractive for money laundering purposes, firstly because the cross-border transfer of funds has been restricted and secondly because cash withdrawals via prepaid cards or other prepaid means of payment have been prohibited. In addition, the prohibition of issuance of anonymous e-money⁶² constitutes yet another deterring factor.

According to the predicate offense breakdown, no money laundering cases have been detected in the e-money sector which implies that the threat level is “Medium Low”.

⁶²Law no. 4446/2016, which entered into effect in March 2017

2.4.4.3. Currency exchange offices

According to the European Commission's Supra-National Risk Assessment, cases have been detected where criminal organisations have used currency exchange offices to convert large amounts of foreign currency into local currency with relative ease and without particular knowledge or technique or vice versa, to acquire large amounts of foreign currency to facilitate criminal activities of an international nature.

Greece has a small number of currency exchange offices. It is worth noting that a large number of illegal migrants or refugees, mainly from Syria, who entered Greece in 2015-2016 and ended up in other EU countries, used the currency exchange offices to convert bank notes from their country of origin.

According to the predicate offense breakdown, individual money laundering cases have been detected in the currency exchange sector and the threat level is "Medium Low".

2.4.4.4. Factoring companies

The factoring of business claims relates to financial services, which are addressed to corporate clients and primarily include the management, collection and financing of short-term collectible trade receivables. The specific nature of the factoring service makes it vulnerable mainly to Trade Based ML typologies, such as transactions with a fake or fictitious value and/or the use of shell companies, which are linked to tax evasion and smuggling offenses (for cross-border transactions).

However, as implied by the lack of specific cases, this is not considered an attractive vehicle for ML purposes, taking into account the limited number of cross-border transactions, as well as the enhanced controls regarding transaction consistencies (e.g. account reconciliation of customers/suppliers, etc).

Based on the above, it arises that the threat level is "Low".

2.4.4.5. Financial leasing companies

Financial leasing companies provide medium to long-term credit services to corporate clients by purchasing assets and leasing these to them. The specific nature of the financial leasing services mitigates the range of the ML typology, which primarily concerns the premature repayment of debts and financial fraud, e.g. via fictitious pricing of the fixed assets that are leased, particularly property.

As it arises from the lack of specific laundering cases, the financial leasing service is not considered an attractive vehicle for ML purposes, taking into account the increased level of controls on fixed assets (valuations from independent assessors, periodical on-the-spot visits to the location of the assets, etc.).

Based on the above, it arises that the threat level is "Low".

2.4.4.6. Credit companies

Credit companies provide credit to natural persons for coverage of their personal needs, mainly via credit cards.

Taking into account the lack of specific laundering cases, the insignificant inherent risk in relation to the size of the sector (rapid drop in activity), and the restricted number of ML typologies, the threat level for this sector is "Low".

2.4.5. Non financial sector

The non-financial sector and especially certain professions that fall into this category, engage in activities that are subject to a High laundering threat. In particular, accountants - tax consultants can be used for the facilitation of tax evasion. As a result, these professions are vulnerable to the risk of laundering.

Notaries, lawyers and real estate agents that mediate in the purchase/sale of property, may contribute in the tax evasion which is a predicate offence of laundering. The data from tax audits revealed that the real property prices were usually and for a long time, especially prior to the economic crises, much higher than the price stated in the sale contract, which coincided with the property's objective value. As a result, buyers paid far less tax than ought to have been attributed.

In addition, the aforementioned professionals are usually used as intermediaries for the laundering of proceeds originating from corruption and illegal drug trafficking, unknowingly on many occasions.

With respect to lawyers, notaries and accountants - tax consultants, the laundering threat is linked with their participation in the formation, operation, or management of companies, given that on occasion the laundering of proceeds from predicate offences (e.g. drug trafficking) is attempted via new or existing businesses.

Dealers of high-value goods are used by criminal groups to launder proceeds from illegal activity, which primarily relates to smuggling or property crimes. The threat level for this sector is classified as "Medium".

In addition, the products of crimes that primarily originate from property crimes are also laundered via pawnbrokers. The threat level for this sector is classified as "Medium".

With respect to gaming, a distinction is made between gaming that is a) land-based and b) online. Specifically:

a) Land-based gambling.

Land-based gambling with the exception of Casinos, favour the player's anonymity and is linked in the past with an increased threat for money laundering. In the years 2011-2014, the player's anonymity while gambling, the absence of a regulatory framework, the provider's extensive network of partners (Physical Network) as well as the absence of regulations, circulars and the internal audit of the latter linked the sector with money laundering cases, primarily from drug trafficking. However, at the end of 2014 the supervisory authority drafted and approved the Regulation which introduced specific obligations for the Providers (preparation and implementation of anti-money laundering policies, organisational measures, record keepings, etc.). This resulted in mitigating the threat for this sector.

With respect to Casinos, their connection with the threat of money laundering, does not concern the ability to integrate the funds into the real economy, given that this is exclusively a cash-intensive sector both while playing and while collecting winnings. Moreover, by law, casinos don't issue winning certificates. Gambling that is conducted in Casinos, although it does not favour anonymity (due diligence is performed on entering the Casino), it facilitates the circulation and exchange of 'dirty' money both for use within the Greek territory as well as outside Greek borders (e.g. foreign players / tourists).

Based on the above, the land-based gambling threat level is classified as "Medium".

b. Online gambling. With respect to online gambling, the threat of money laundering concerns their interconnection with crimes of fraud, corruption, bribery and organised crime (e.g. via the fixing of sports

events and betting on these) combined with the supervisory authority's remote control due to the providers being established abroad. Also, online gambling is linked with the illegal gambling in internet cafes or other catering venues (illegal land-based network), via special access codes in the name of the organisation's members (not individually per player) and the use of specific means of payment which either favour the holder's anonymity, or constitute part of the illegal network. The above phenomena escape the Hellenic Gaming Commission's scope of responsibility, which is restricted to granting its assistance to the competent law enforcement and public prosecutor authorities (economic police, cyber crime, FIU, public prosecutors, interrogators, etc.). In addition, the legal online gambling network is regulated by decision 129/2/7.11.14 (B 3162) issued by the Hellenic Gaming Commission, and introduced specific requirements for the providers (preparation and implementation of anti-money laundering policies, organisational measures, STRs, record keeping, etc.). Finally, it is noted that participation in the above games is exclusively carried out via institutions of the financial sector and to this day there is no record of online gambling laundering cases. Based on the above, the online gambling threat level is classified as Medium-Low.

With respect to certified auditors, the threats that could exist from this profession include:

1. Wrongful exercise of the certified auditor-accountant's duties (voluntary or involuntary). Specifically, if the auditor does not display the due diligence and the required professional scepticism in investigating indicators that may reveal possible unlawful actions.
2. The audit firms' internal organisational structure may not meet the requirement of the International Standard on Quality Control (ISQC) 1, whose purpose is to establish and maintain a quality control system that will provide judicious assurance that the audit firm and its personnel comply with professional standards and the applicable legal and regulatory requirements.

The threat level for the sector is assessed as "Medium".

3. NATIONAL VULNERABILITY

3.1. Summary

The Risk Assessment of Laundering of the proceeds of crime is based on the analysis of the threats and the vulnerability of the National Mechanisms. The assessment of national combating ability of ML (defence and reaction mechanisms in ML) and any other deficiencies or vulnerabilities in the various sectors of the economy (National Sectoral Vulnerability) determine the national vulnerability assessment.

In this chapter, Greece's weaknesses/deficiencies are determined with regard to combating laundering of the proceeds of crime. Also national actions are proposed, in the legislative and the operational framework, which will lead to the establishment of a national strategy in combating ML. The National Vulnerability Assessment contributes in prioritising the required actions and arrangements and to ensuring efficient allocation of national resources through the national strategic plan.

3.2. National ML combating ability factors

The evaluation of the input variables of national ML combating ability factors (defence and reaction mechanisms to ML), is based on data and information pertaining to the last five (5) years, relying on national and mainly international statistics, surveys, reports from international organizations, institutions, working groups, articles and reports, and by utilizing the criteria based on the methodology of the World Bank as the main tool, has resulted in the following grading and prioritisation of the variables.

	ASSESSMENT RATING	
A. INPUT VARIABLES/NATIONAL ML COMBATING ABILITY FACTORS		
Quality of AML Policy and Strategy	[0.5] Medium	0,5
Effectiveness of ML Crime Definition	[0.7] High	0,7
Comprehensiveness of Asset Forfeiture Laws	[0.6] Medium High	0,6
Quality of FIU Intelligence Gathering and Processing	[0.6] Medium High	0,6
Capacity and Resources for Financial Crime Investigations (incl. AF)	[0.6] Medium High	0,6
Integrity and Independence of Financial Crime Investigators (incl. AF)	[0.6] Medium High	0,6
Capacity and Resources for Financial Crime Prosecutions (incl. AF)	[0.5] Medium	0,5
Integrity and Independence of Financial Crime Prosecutors (incl. AF)	[0.7] High	0,7
Capacity and Resources for Judicial Processes (incl. AF)	[0.4] Medium Low	0,4
Integrity and Independence of Judges (incl. AF)	[0.7] High	0,7
Quality of Border Controls	[0.5] Medium	0,5
Comprehensiveness of Customs Regime on Cash and Similar Instruments	[0.8] Very High	0,8
Effectiveness of Customs Controls on Cash and Similar Instruments	[0.5] Medium	0,5
Effectiveness of Domestic Cooperation	[0.6] Medium High	0,6
Effectiveness of International Cooperation	[0.7] High	0,7
Formalization Level of Economy	[0.5] Medium	0,5
Level of Financial Integrity	[0.6] Medium High	0,6
Effectiveness of Tax Enforcement	[0.6] Medium High	0,6
Availability of Independent Audit	[0.7] High	0,7
Availability of Reliable Identification Infrastructure	[0.5] Medium	0,5
Availability of Independent Information Sources	[0.6] Medium High	0,6
Availability and Access to Beneficial Ownership Information	[0.4] Medium Low	0,4

Table8- Table of variables of national vulnerability for ML

PRIORITY RANKING FOR INPUT VARIABLES/NATIONAL ML COMBATING ABILITY FACTORS	Priority Ranking
Quality of AML Policy and Strategy	1
Effectiveness of ML Crime Definition	
Comprehensiveness of Asset Forfeiture Laws	9
Quality of FIU Intelligence Gathering and Processing	11
Capacity and Resources for Financial Crime Investigations (incl. AF)	3
Integrity and Independence of Financial Crime Investigators (incl. AF)	4
Capacity and Resources for Financial Crime Prosecutions (incl. AF)	2
Integrity and Independence of Financial Crime Prosecutors (incl. AF)	
Capacity and Resources for Judicial Processes (incl. AF)	5
Integrity and Independence of Judges (incl. AF)	
Quality of Border Controls	14
Comprehensiveness of Customs Regime on Cash and Similar Instruments	
Effectiveness of Customs Controls on Cash and Similar Instruments	10
Effectiveness of Domestic Cooperation	12
Effectiveness of International Cooperation	
Formalization Level of Economy	7
Level of Financial Integrity	15
Effectiveness of Tax Enforcement	13
Availability of Independent Audit	
Availability of Reliable Identification Infrastructure	7
Availability of Independent Information Sources	16
Availability and Access to Beneficial Ownership Information	6

Table9- Priority ranking for input variables

3.3. National sector vulnerability

Based on the methodology of the World Bank for determining the level of vulnerability per sector, and by the use of the “weighted approach” option, the overall national sectoral vulnerability is identified to be 0.55"Medium,". By the same way the overall prioritization (according to the vulnerability) of the sectors is determined and priorities for actions is set, as illustrated in the following:

SECTORS	FINAL VULNERABILITY SCORE	WEIGHTS	PRIORITY RANKING
BANKS	0,51	10	4
LIFE INSURANCE COMPANIES	0,36	6	14
LEASING COMPANIES	0,18	3	
FACTORING COMPANIES	0,21	4	
MONEY REMMITTERS	0,68	4	5
E-MONEY INSTITUTIONS	0,47	3	13
BUREAUX DE CHANGE	0,40	2	15
INVESTMENT SERVICES COMPANIES	0,54	5	7
FUND AND ASSET MANAGEMENT COMPANIES	0,27	4	
PORTFOLIO INVESTMENT COMPANIES	0,16	1	
RECEIVAL AND TRANSMISSION OF ORDERS COMPANIES	0,16	1	
LAND BASE GAMBLING SERVICES	0,70	6	3
ONLINE GAMBLING SERVICES	0,56	3	11
ACCOUNTANTS	0,83	5	2
AUDITORS	0,54	3	12
NOTARIES	0,80	3	6
REAL ESTATE AGENTS	0,77	2	9
LAWYERS	0,86	5	1
DEALERS IN HIGH VALUE GOODS	0,72	2	10
PAWN BROKERS	0,78	2	8

Table10- Overall national sectoral vulnerability

3.4. National Vulnerability

By correlating the result for overall national sectoral vulnerability (Overall Sectoral Money Laundering Vulnerability) and the capability of national defence and reaction mechanisms for ML (National Money Laundering Combating Ability), the level of national vulnerability to ML is identified to be 0.52 and is deemed "Average".

Relevant graphs have been provided, as well as the relevant National Vulnerability Map, which result from the World Bank's methodological tool.

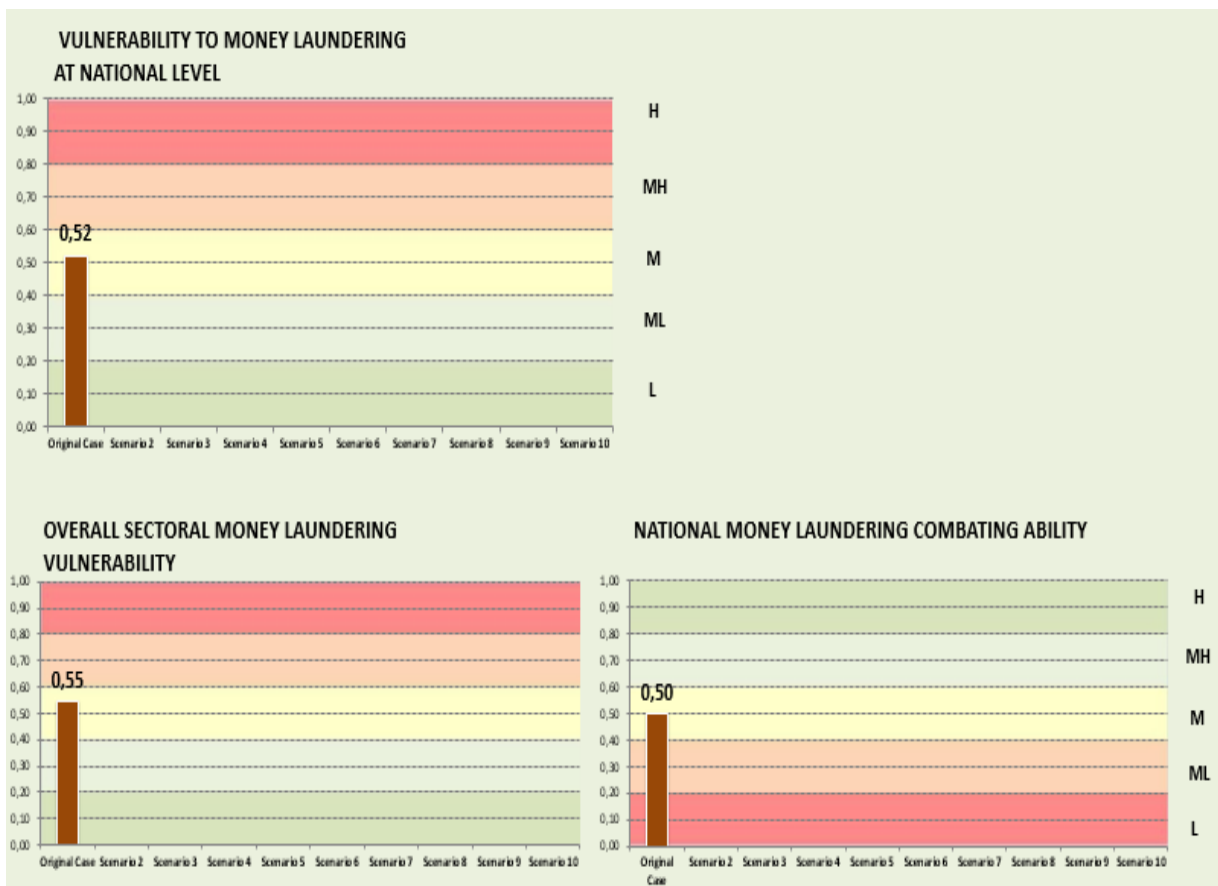


Table11-National vulnerability graphs

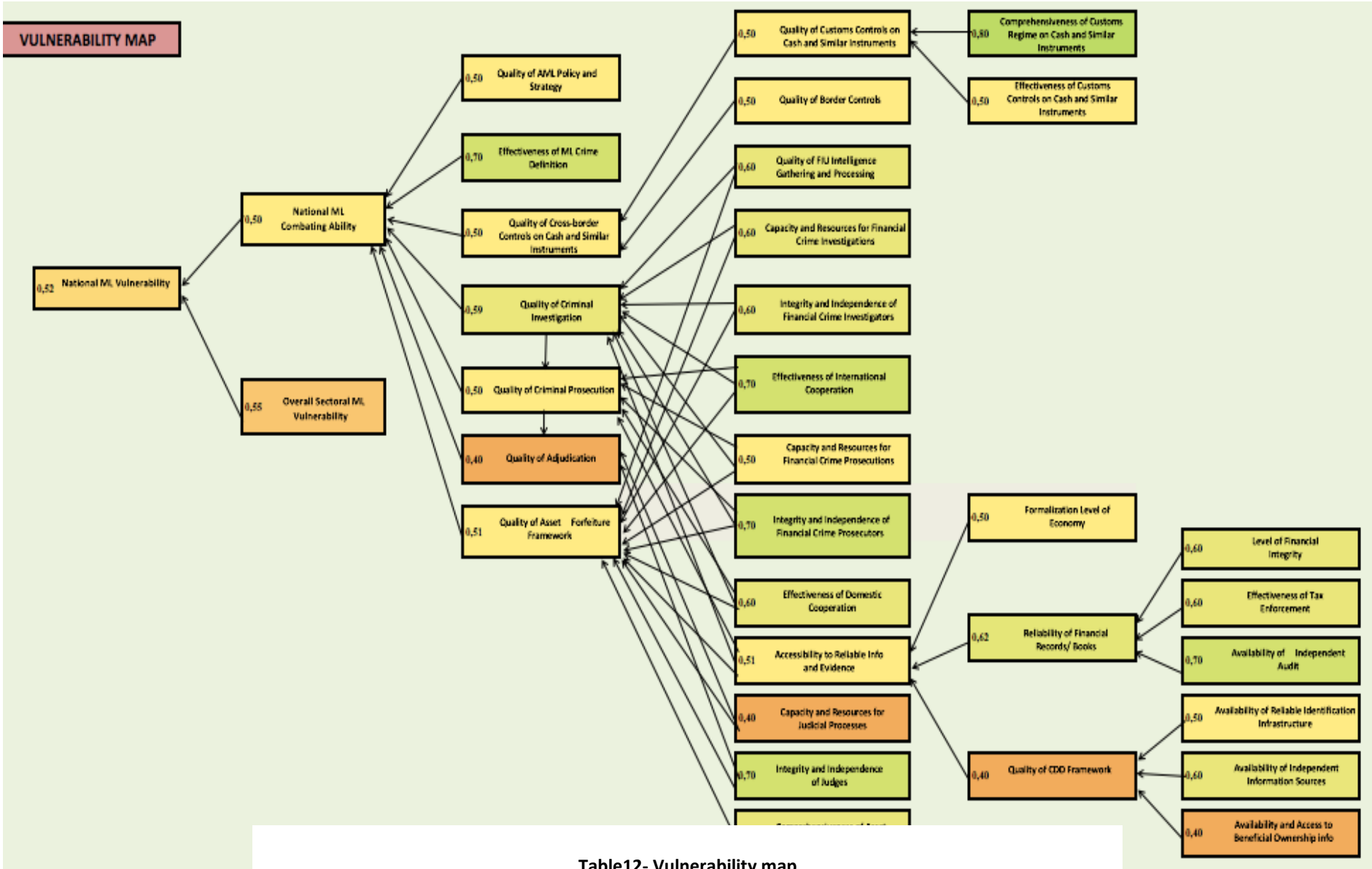


Table12- Vulnerability map

3.5. National ML combating ability factors

3.5.1. Quality of AML policy and strategy

Assessment rating: Medium (0.5)

In Greece, the national strategy to combat ML/TF is presently in the stage of drafting and adoption of best practices.

The first three European Commission Directives have been transposed into the Greek legal system⁶³, taking into account the recommendations of the FATF for combating ML/TF. The 4th EU Directive 2015/849/EC is expected to be transposed into national law within the second quarter of 2018.⁶⁴

The Ministry of Finance acts as a central coordinating body for implementation of the provisions of the law on combating ML/TF, evaluation and improvement of the effectiveness of the relevant mechanisms, and coordination of the actions of the competent authorities. The Ministry of Finance has set up a Strategy and Policy Elaboration Committee for combating ML/TF. The Strategy Committee is chaired by a political figure, namely the current Secretary General of Economic Policy of the Ministry of Finance, and is composed of senior officials of the organisations involved⁶⁵.

Its main objective is to prepare and design specific policies to deal with identified weaknesses in the country's general mechanism, with the goal of preventing ML/TF. To achieve this goal, among other things, it monitors international developments while taking into account the recommendations of international organizations and bodies (FATF, UN, etc.), it cooperates with national bodies and the Authority⁶⁶ and develops initiatives for partnerships with the private sector. Its work is presented to the Parliamentary Committee on Institutions and Transparency through the annual activity report submitted at the beginning of the following year.

The Strategy Committee, despite the fact it has held only a limited number of meetings, has stepped up actions, subsequent to the amendment of Article 9 of Law 3691/2008, which occurred through Article 57 of Law 4370/2016 (Government Gazette A' 37), over the last two years (2016-2017), for the formulation and consistent implementation of a strategy for combating ML/TF. In view of the national evaluation by the F.A.T.F. and the obligations stipulated by the 4th Directive, the Strategy Committee proceeded with the establishment of:

A. Eight (8) special working groups composed of specialised officials of the organizations involved for the purpose of preparing the 1st National Risk Assessment Report.⁶⁷

⁶³Through Law 2331/1995 Directive 91/308/EEC was transposed, through Law 3424/2005 Directive 2001/97/EC was transposed, and through Law 3691/2008, which replaced Law 2331/1995, Directives 2005/60/EC were transposed. Law 3691/2008 has been amended through Law 3932/2011, Law 4389/2016, Law 4478/2017 and Law 4506/2017.

⁶⁴The draft law for transposition of Directive 2015/849 is already in public consultation.

⁶⁵(a) the Ministry of Finance (Directorate General for Economic Policy, Directorate General for Taxation, Directorate General for Customs and Excise Duties and Financial Crime Prosecution Unit), (b) Ministry of Interior and Administrative Reconstruction (Greek Police Headquarters), (c) Ministry of Foreign Affairs, (d) Ministry of Justice, Transparency and Human Rights (General Secretariat for Combating Corruption), (e) Ministry of Economy, Development and Tourism; (f) Ministry of Shipping and Island Policy (Coast Guard Headquarters), (g) The Authority for Anti-money Laundering and Combating the Financing of Terrorism and Auditing of Asset Declarations, (h) Bank of Greece (i) Securities and Exchange Commission, (j) Hellenic Accounting and Auditing Standards Oversight Board (j) Hellenic Gaming Commission

⁶⁶Article 7 of Law 3691/2008 provides for operation of the Committee for Anti-money Laundering of the Proceeds of Crime and Combating the Financing of Terrorism which was renamed, through the amendment of Law 3932/2011, the "The Authority for Anti-money Laundering of the Proceeds of Crime and Combating the Financing of Terrorism, and Auditing of Asset Declarations

⁶⁷Decisions of the Secretary General of the Directorate General of Economic Policy, Directorate of Fiscal Policy, Group 1 "Assessment of the Threat of Money Laundering": Directorate General of Economic Policy Ref. No. 0000588 EΞ 2017/ΧΠ 624/06-04-2017 (Amended Directorate General of Economic Policy Ref. No. 0001178 EΞ 2017/ ΧΠ1264/02-08-2017), Group 2 "Assessment of Vulnerability for Money Laundering:" Directorate General of Economic Policy Ref. No. 0001829 EΞ2017/ΧΠ 2092/04-12-2017 (Amended Directorate General of Economic Policy Ref. No. 0001179 EΞ 2017/ΧΠ 624/02-08-2017 0001485 EΞ 2017/ΧΠ 1675/06-10-2017, Group 3: Directorate

B. Drafting group of the NRA for the purpose of homogenising the individual projects of the aforementioned groups and drafting of the final version of the NRA.⁶⁸

C. Permanent Support Group of the Strategy Committee's work and

D. Monitoring and support group for the national evaluation by the F.A.T.F.

Completion of the NRA with the proposed actions will contribute to the creation of a single national strategic plan against ML/TF

At the same time, the organisations involved, officials of which participate on the Strategy Committee, within the context of their responsibilities, shall adopt policies, strategies and action plans against ML/TF with relevant directives, circulars, reports, workshops and updates.⁶⁹ It should be noted that, in this context, the Greek Police prepares an annual report on serious and organised crime, configures an anti-crime policy program (every four years), while in 2013 it also prepared a policy for dealing with financial crime following an assessment by, and at the recommendation of, GENVAL, aiming for this to constitute the core of national policy, placing particular emphasis on and giving priority to combating ML/TF.

3.5.2. Effectiveness of ML crime definition

Assessment rating: High (0.7)

Greece's main law for ML/TF is Law 3691/2008 harmonised with the relevant European Directives, whereas its amendment is expected upon incorporation of the 4th Directive 2015/849/EC.

Individual issues have been dealt with through changes in the legal framework, examples of which include:

- Law 3842/2010 containing Article 77, in which the following were added as predicate offenses: (a) tax evasion, smuggling,
- Law 3875/2010 on the criminalisation of the offense of ML (amendment 187A Greek Penal Code),
- Law 3932/2011 on the legal form and structure of the Authority, and provisions were introduced which outline procedures for the freezing of assets of persons, groups or entities which are subject to specific economic sanctions.
- (Law 4170/2013, through Article 74, defines measures for increased due diligence in the Regional Operation Programs that are established in Greece,

General of Economic Policy Ref. No. 0000431 ΕΞ 2017/ΧΠ 429/16-03-2017, Group 4: Directorate General of Economic Policy Ref. No. 0000430 ΕΞ 2017/ΧΠ 430/16-03-2017 (Amended Directorate General of Economic Policy Ref. No. 0000780 ΕΞ 2017/ ΧΠ. 842/18-05-2017), Group 5: Directorate General of Economic Policy Ref. No 0000429 ΕΞ 2017/ΧΠ 431/16-03-2017, Group 6: Directorate General of Economic Policy Ref. No. 0000428 ΕΞ 2017/ΧΠ 432/16-03-2017, Group 7: Directorate General of Economic Policy Ref. No. 0000427 ΕΞ 2017/ΧΠ 433/16-03-2017, Group 8: Directorate General of Economic Policy Ref. No. 0000589 ΕΞ 2017/ΧΠ 626/06-04-2017 (Amended Directorate General of Economic Policy Ref. No 0000589 ΕΞ 2017/ ΧΠ626/06-04-2017& Directorate General of Economic Policy Ref. No. 0001181 in 2017/ HP1266/02-08-2017).

Directorate General of Economic Policy Ref. No. 0000551 ΕΞ 2018/ΧΠ 476/06-03-2018 Decision of the Secretary General of the Directorate General of Economic Policy / Directorate of Fiscal Policy.

⁶⁹The Bank of Greece, the Securities and Exchange Commission and the Hellenic Gaming Commission impose, on the persons supervised by them, a policy for combating ML/FT Specifically, Special Secretariat of the Financial and Economic Crime Unit : Ref. No. 12572/2834/10-12-2010, Ref No. 5205/23-07-2015, Port Authority Ref. No. 1000.0/63979/2017, Independent Authority for Public Revenue/33rd Directorate of Customs Offices:Δ33B5041293/05-10-2011, Δ33B5012421 ΕΞ2014/ 23-05-2014), Authority: Ref. No. 3734/2017, Ref. No. 4690/2017, Ref. No 5551/2017, Bank of Greece: ΕΤΠΘ 281/17.03.2009, Securities and Exchange Commission: Decision 1/506/2009, Independent Authority for Public Revenue/Directorate General of Tax Administration. : Government Gazette Β' 605 / 7- 5 – 2010, ministerial circular 1127/31-08-2010, ministerial circular 1196/16-10-2012, ministerial circular 1185/23-07-2013, ministerial circular 1067/05-04-2017, Bulletin D 1191051 EX 2017/20-12-2017. Greek Police Decree No. 1507/171908154

- (Law 4174/2013 whereby non-payment of debt to the State was added as a Predicate Offense for ML (Art. 68, par. 1) and the obligation is introduced of verification of clients' incomes by the supervised institutions, on the basis of a salary statement (Article 68, par. 7)
- Law 4370/2016, through Article 57, amended Article 9 of Law 3691/2008 with regard to the Strategy Committee,
- Law 4389/2016 whereby issues related with the submission of financial situation reports to Unit C of the Authority, as well as issues related to the Authority's staffing procedures are laid out,
- Law 4478/2017 "Penalties and adaptation of the Greek legislation on laundering, search, seizure and confiscation of proceeds of crime and the financing of terrorism and other provisions" (*Warsaw Convention*) with the resulting amendments to Law 3691/2008⁷⁰.
- Law 4506/2017 (A' 191), Article 51 "Liability of legal persons" of Law 3691/2008 was replaced by Article 6.

Article 2 of Law 3691/2008 stipulates that, for laundering of proceeds of crime, a connection is required with a specific predicate offense, as well as acquisition of an illegal pecuniary benefit. The definition of a predicate offense includes the main forms of serious and organised crime as well as tax offenses.⁷¹ The concept of offense includes both participation and providing assistance, as well as self-laundering.

Money Laundering constitutes a separate offense and can be prosecuted independently of criminal prosecution and conviction for the predicate offense.⁷² Criminal penalties are imposed on natural persons for the offense of ML. They are proportionate with the penalties imposed for the predicate offence and independent of it.⁷³ These include a wide range of sanctions, both administrative and civil. Sentences Fines⁷⁴ can also be applied. Administrative and civil sanctions are imposed on legal persons, independent of the civil, disciplinary or criminal liability of natural persons.⁷⁵ Penalisation applies to all the elements of the Vienna⁷⁶ and the Palermo Convention.⁷⁷

The legal vacuum in the imposition of penalties on legal arrangements that have or not, acquired a legal personality, has been filled by article 6 of law 4506/2017⁷⁸. In addition, the possibility for imposing sanctions, is provided for all cases, in which predicate offenses outlined in Law 3691/2008 have been

⁷⁰ Law 3691/08), Article 45 par. 1 "Criminal Penalties", Article. 46 par. 1 "Confiscation of Property", Article 47 "Compensation to the State", Article 48. Par. 2, 6 and 7 Freezing and prohibition of divestiture of assets"

⁷¹ Law 3691/2008, Article 3 and Law 3842/2010 Article 77.

⁷² Law 3691/2008, Article 45 par. 2

⁷³ Law 3691/2008, Article 45.

⁷⁴ see the case "Electricity Supply Companies". Decisions No. 534/07-02-2017, 599/10-02-2017, 1115/07-03-2017, 446/15, 675/15, 746/15, 825^A /15, 1860^A /15, 1969/15, 2846^A /15, 2959/15, 3031/15, 3186/15, 3554/15, 279^A/16, 689/16, 977/16, 1223^A/16, 1391/16, 2703/16 of the Three-member Court of Appeal for Felonies (as entered in the Special Register on 17-07-2017 and assigned number 2828). The sentences handed down by the Court to 11 defendants are as follows: **1st Defendant**, a combined prison sentence of 21 years for acts of embezzlement, money laundering and smuggling, and a fine of 1.5 million euros. **2nd Defendant**, a combined prison sentence of 14 years and a fine of one (1) million euros for the offenses of embezzlement, smuggling and money laundering. **3rd Defendant**, a prison sentence of 10 years for the offense of aiding and abetting embezzlement. **4th and 5th Defendants**, a prison sentence of 15 years for all three offenses and a fine of 500,000 euros. **6th Defendant** a prison sentence of 7 years for the offense of money laundering. **7th Defendant**, a prison sentence of 4 years and a fine of 500,000 euros for the act of money laundering, **8th Defendant**, a prison sentence of 7 years and a fine of 300,000 for money laundering **9th Defendant** a prison sentence of 10 years and a fine of 300,000 euros for money laundering, **10th Defendant** a prison sentence of 10 years and a fine of 300,000 euros for money laundering, and **11th Defendant** a prison sentence of 4 years and a fine of 50,000 euros for the act of money laundering.

⁷⁵ Law 3691/2008, Article 51, as amended by Law 4506/2017.

⁷⁶ Vienna International Convention against illicit traffic in narcotic drugs and psychotropic substances, which was ratified by Greece through Law 1990/1991 (Government Gazette A' 193/1991)

⁷⁷ The United Nations Convention against Transnational Organized Crime (Palermo, 2000), which was ratified by Greece through Law 3875/2010 (Government Gazette A' 158/2010)

⁷⁸ In accordance with Directive (EU) 2015/849 (4th EU Directive)

committed. Also in the same article, the penalties foreseen, have increased significantly. The Special Secretariat of the Financial and Economic Crime Unit, and specifically the competent operational directorate of the latter, was designated as the competent authority for the imposition of administrative penalties on non-liable legal persons or entities that commit the punishable acts of ML, or any of the predicate offenses, when these are committed for the benefit or on behalf of a legal person or entity.

3.5.3. Comprehensiveness of asset forfeiture laws

Assessment rating: Medium High (0.6)

Greece possesses a comprehensive legal framework⁷⁹ for freezing, seizing and confiscating the proceeds of crime and the products of crime, especially subsequent to the adaptation of the Greek legislation to the Warsaw Convention.

With regard to seizure, the investigative magistrate and investigative officials proceed with seizures of money or objects related to the crime under investigation as means of its commission or products of the latter.⁸⁰

Similarly, the Prosecutor for Financial Crime⁸¹ and the President of the Authority⁸² proceed with freezing of accounts, securities and financial products, safety deposit boxes, and other assets. The possibility of freezing of bank accounts and assets represents a special case, which is imposed as a preventative measure by the Head of the competent Regional Directorate of the Special Secretariat of the Financial and Economic Crime Unit⁸³, regarding which forthcoming legislation is expected for harmonisation with the requirements of the Constitution.⁸⁴

With regard to confiscation, the judicial authorities shall confiscate assets that are products of felonies or misdemeanors stemming from deceit, their value, of those obtained directly or indirectly through these, and any objects used, or intended to be used, in the execution of or attempt at such an act, if these belong to the perpetrator or one of his or her accomplices⁸⁵. Confiscation is imposed even if the assets or means belong to a third party, provided that the latter knowingly committed a predicate offense, or the offenses of ML/TF, at the time of their acquisition.⁸⁶ For confiscation, a conviction or ruling by a competent judicial council is required, even if no prosecution took place due to the death of the perpetrator, or the prosecution ceased definitively or was declared inadmissible.

⁷⁹ see Annex Tables 1-3: Illustration of a legal framework for Seizure - Freezing - Confiscation

⁸⁰ Greek Code of Criminal Procedure Article 260 and Law 3691/2008 Article 48

⁸¹ Law 2523/1997 Article 17A. It should be noted that par. 8 of Article 17 A of Law 2523/1997 has been amended in adaptation to the recent case-law of the Council of State (Decisions No. 3316/2014 and 1260/2015 of the CoS,) which led to certain issues related to the powers of the officials of the Special Secretariat of the Financial and Economic Crime Unit to proceed with preventative freezing, in accordance with 30 of Law 3296/2004.

⁸² Law 3691/2008 Article 48 par. 5

⁸³ Law 3296/2004 Article 30 par. 5 scenario E

⁸⁴ Decisions No 3316/2014 and 1260/2015 of the CoS.

⁸⁵ Hellenic Penal Code Article 76

⁸⁶ see the case "Electricity Supply Companies". Decisions No. 534/07, 599/10-02-2017-02-2017, 1115/07-03-2017, 446/15, 675/15, 746/15, 825^A/15, 1860^A/15, 1969/15, 2846^A/15, 2959/15, 3031/15, 3186/15, 3554/15, 279^A/16, 689/16, 977/16, 1223^A/16, 1391/16, 2703/16 of the Three-member Court of Appeal for Felonies. More than €120 million has been frozen, while it was decided to turn over €59 million to the State (which for the most part pertains to extraordinary special levies on buildings connected to the power grid as well as interest) and approximately €30 million to the Local Government. (related to debt) Likewise, see Corruption Case (passive corruption) and money laundering involving, inter alia, a political figure (former Minister): First instance Decisions No. 2384, 2471, 2474, 2531, 2532, 2754, 2892, 2893 Transition, 2961, 3298, 3582, 3827, 3932, 3960, 3961, 3986, 4097, 4129, 4130, 4132, 4137 and 4554/2013 of the Three-member Court of Appeal for Felonies, in which, inter alia, a large number of assets were confiscated (movable and immovable property).

The full statistics related to seizure and confiscation⁸⁷ are provided in the table below for the years 2016-2017:

TOTAL REPORTED SEIZURES (I.A.P.R. – D.M.P.M.⁸⁸)		
OFFENCES	2016	2017
FRAUD - FORGERY	172	100
PARTICIPATION IN CRIMINAL ORGANIZATION	375	279
THEFT AND ROBBERY	1237	584
SMUGGLING	106	112
SMUGGLING OF IMMIGRANTS	481	185
DRUGS AND ARMS	455	253
RECEIVE AND DISTRIBUTION OF CRIME PRODUCTS	60	20
VIOLATIONS OF CUSTOMS CODE	198	95
GAMING VIOLATIONS	245	194
SUM	3329	1822

Table13- Total reported seizures

⁸⁷Seizures reported to the Directorate for Management of Public Material of the Independent Authority for Public Revenue for the years 2016-2017.

⁸⁸Directorate for Management of Public Material of the Independent Authority for Public Revenue

TABLE OF FROZEN BANK ACCOUNTS ⁸⁹

REGULATOR/ AUTHORITY OF SEIZURE	2014			2015			2016		
	BANKS		INSURANCES	BANKS		INSURANCES	BANKS		INSURANCES
	€	USD	€	€	USD	€	€	USD	€
Judiciary Provisions (article 48 of Law 3691/2008) Freezing of bank accounts by financial crime prosecutor, magistrate (Law. 4022/2011) e.t.c	42.295.634	362.764	1.180.791	133.689.160	939.227	2.286.725	176.441.558	991.857	2.502.382
Authority's decisions	212.147.244	50.106	583.965	203.030.119	50.111	448.359	210.223.820	50.116	450.187
Decisions by tax or custom authorities / Ensuring of public interest	35.244.182	3.573	190.970	68.994.032	4.576	215.575	75.196.626	4.576	438.268
TOTAL	289.687.060	416.445	1.955.728	405.713.311	993.915	2.950.660	461.862.004	1.046.550	3.390.838

Table14- Frozen bank accounts

⁸⁹ Data from the Bank of Greece 2014-2016. .

CAPITAL MARKET COMMISSION		Euro
2014	Judicial authorities	5.525.824,84
	Authority	3.950.527,24
	Custom and Tax authorities	4.571.457,22
2015	Judicial authorities	16.712.929,52
	Authority	4.121.030,17
	Custom and Tax authorities	8.980.704,64
2016	Judicial authorities	33.739.260,90
	Authority	4.338.887,64
	Custom and Tax authorities	9.993.153,94
TOTAL		91.933.776,11

Table15- Capital market freezes

By Joint Ministerial Decision No. 24296 fin. /29-03-2018 of the Ministers of Justice, Transparency and Human Rights, and the Minister of Finance (Government Gazette B' 1302/13-04-2018), issued by means of delegated acts in accordance with Articles 5 and 32 of Law 4478/2017, the Special Secretariat of the Financial and Economic Crime Unit is designated as the competent institution for the management of confiscated and frozen assets. Management may include their use for the public interest, for social purposes, or to compensate the victim, as well as for the effective management of assets frozen in view of possible confiscation. Efficient management of the frozen assets includes the possibility of their sale or transfer, when this is deemed necessary to safeguard their economic value. Competence was bestowed upon the same Service (Special Secretariat of the Financial and Economic Crime Unit), through the aforementioned JMD, to maintain and process statistics related to frozen and confiscated assets.

A bank account of the Greek State is maintained with the Bank of Greece, in which sums are deposited that result from crime against it and represent revenue of the State Budget for financing of projects or actions, particularly training, research, health or social solidarity, pursuant to a decision by the Minister of Finance.⁹⁰⁹¹

⁹⁰ Article 180 of Law 4270/2014.

3.5.4. Quality of FIU intelligence gathering and processing

Assessment rating: Medium High (0.6)

The Authority is one of the independent authorities of Greece and operates as the national unit responsible for combating money laundering and terrorist financing (ML/TF), as well as for conducting source of funds investigations.⁹² The Authority is chaired by an active Public Prosecutor to the Supreme Court appointed by the Supreme Judicial Council, whereas its Members are approved by the Parliament's Permanent Committee on Institutions and Transparency.⁹³ The assignment and investigation of the cases, as well as the freezing of the respective assets⁹⁴ require a decision of the Chair and the Plenary.⁹⁵ The banking, financial, tax and professional secrecy does not apply for the investigations and inquiries conducted by the Authority. Within the same scope, the Authority has been granted with direct access to all kinds of data preserved and processed by any other public institution or organisation, such as the Bank Account Registry System and the Tiresias System.⁹⁶ The Chair, the Members and the staff of the Authority are bound by the principles of objectivity, impartiality and confidentiality. The Authority consists of three (3) individual Units, with distinct competences, staff and infrastructure, which may cooperate on common cases under certain circumstances.⁹⁷ Specifically:

1st Unit: Financial Intelligence Unit (FIU) (Chair and eight (8) Members of the Authority), which is responsible for evaluating and investigating both reports on suspicious or unusual transactions (STRs), and any information regarding ML/TF deriving from either domestic or foreign sources.⁹⁸

2nd Unit: Financial Sanctions Unit (FSU) (Chair and two (2) Members of the Authority), which is responsible for identifying natural and legal persons or entities related to terrorism, as well as for imposing the UN Security Council Regulations and the EU Decisions concerning restrictive measures (asset freezing).⁹⁹

⁹¹Decisions of the Minister of Finance (a) 2/72673ΔΠΓΚ (Government Gazette B, 2736/2014), (b) 2/67683ΔΠΓΚ (Government Gazette (B, 2641/2015), and (c) 2/67683ΔΠΓΚ (Government Gazette (B, 3340/2017)

⁹²Law 3691/2008 Article 7, as amended with Law 3932/2011 Article 13 (6)

⁹³The Members of the Authority and their substitutes are appointed by a joint decision of the Minister of Justice, Transparency and Human Rights and the Minister of Finance, following a recommendation pro rata to their competence by of the Ministers of Justice, Transparency and Human Rights, Finance, Exterior and Citizen Protection, the Governor of the Bank of Greece and the Board of Directors of the Hellenic Capital Market Commission, who recommend persons that stand out for their scientific background, their integrity and professional skills and experience in the banking, financial, legal or business sector, depending on the requirements of the separate Units of the Authority. Ordinary members are appointed following an opinion of the Permanent Committee of Institutions and Transparency of the Parliament on the suitability of the recommended individuals. For this purpose, the procedure of paragraphs 3 through 5 of Article 49A of the Regulation of the Parliament applies mutatis mutandis, which is initiated at the initiative of the Minister of Justice, Transparency and Human Rights.

⁹⁴ When the 1st Unit is carrying out an investigation, the President of the Authority may issue a decision ordering the prohibition of any transactions of accounts, securities, financial products or the opening of safety deposit boxes or the prohibition of transfer or sale of any other asset, under the terms and conditions provided for by Article 48 of Law 3691/2008 as presently in force.

⁹⁵ Decision 38865/B1208 Ministry of Finance

⁹⁶For this reason all of the Authority's Units have direct access to the TAXIS, ELENXIS, ETAK applications as well as other applications of the Ministry of Finance and the Independent Authority for Public Revenue, as well as online applications of the Police (POLICE ON LINE). The Units may request in the framework of their audits and investigations the cooperation and provision of all types of information from natural persons, judicial, preliminary investigation or investigation authorities, public services, legal persons governed by public or private law and organisations of any form. The Units moreover, in cases they consider serious, may conduct special on-site audits at any public service or at organisations and businesses of the public sector, cooperating, as necessary, with the competent authorities in each case. The Units ask the liable persons (Banks, Insurance Companies, etc.) to provide all the information requested for the fulfilment of their duties, which include grouped information pertaining to certain categories of transactions or activities of domestic or foreign natural or legal persons or entities. Moreover, they can carry out on-site inspections at the facilities of the liable persons, on condition of compliance - if applicable - with Articles 9, paragraph 1, 9A and 19 paragraph 1 of the Constitution, and inform all competent authorities about cases of lack of cooperation or non-compliance of these persons with their obligations, in accordance with this law.

⁹⁷Law 3691/2008 article 7C para. 5.

⁹⁸Law 3691/2008 Article 7A .

⁹⁹See "Risk Assessment and Vulnerability for Terrorism Financing Report - Module 8 NRA)

3rd Unit: Source of Funds Investigation Unit (SFIU), (Chair and four (4) Members of the Authority), which is responsible for receiving and auditing asset declarations of specific categories of individuals¹⁰⁰.

At this point it is deemed worth mentioning that according to paragraph 3.6.3 of the evaluation report on the fifth round of mutual evaluations of the EU Council (Brussels 24 May 2012, 7614/12/REV2, GENVAL 1) on “Financial Crime and Financial Investigations”, one of the three units of the Authority (namely the 3rd Unit) has the potential to develop into an EU “best practice”. According to the same evaluation report, Greece is the only EU Member State that has properly integrated a comprehensive personal financial disclosure system for PEPs into its FIU (which simultaneously investigates ML and TF).¹⁰¹

The Authority holds an independent budget financed by the Ministry of Finance, whereas it is staffed by scientific, administrative, and scientific personnel, seconded by Ministries and Agencies on the basis of their distinguished knowledge and skills. The personnel is subject to annual evaluation and attends trainings, both in Greece and abroad takes part in trainings in Greece and abroad.¹⁰² During the recent years, the Authority has been understaffed, while long delays in the staffing process have also been observed.

The Authority has a state of the art IT system which enables the digitisation, electronic forwarding and reception of documentation, STRs and other information submitted by the majority of the obligated persons. This electronic system enables the management and correlation of the information received by the Authority.

Suspicious Transaction and Information Reports¹⁰³

Year	2014	2015	2016
Total number	15.746	23.559	6.295
Derivation			
Banks	5.513	2.536	1.492
Insurance Companies	254	540	713
Securities	59	83	48
Bureaux de change	235	9	16
Money remitters	7.962	4.575	480
Public services and organizations	1.567	15.639 *	3.254
Complaints by individuals	143	162	71
Other	13	15	221

Table16- Suspicious transaction and information reports

¹⁰⁰Law 3213/2003 Article 3 para. 1 point aa, except for those of Article 14 of the same law.

¹⁰¹<https://www.eumonitor.nl/9353000/1/j9vvik7m1c3gyxp/vizt6xl5rfzz>

¹⁰² See Annual Reports of the 1st Unit of the Authority: http://www.hellenic-fiu.gr/index.php?option=com_content&view=article&id=72&Itemid=142&lang=el

¹⁰³The majority of reports, which mostly come from the IPRA's Services and Credit Institutions, following prioritisation and evaluation, are investigated as cases. Based on the effective analysis and processing of cases, there has been a large number of freezing with the corresponding criminal product per year, for which the competent local Court of First Instance Prosecutor has been directly informed. The large number of suspicious transaction reports in 2014 and 2015 is due to: a. the large number of reports from the Tax Offices due to article 68 par. 1 of Law 4174/1993, which added to the basic offences of money laundering and terrorist financing of Law 3691/2008, the offence of non-payment of debts to the State and the circular dated 23/12/2014 of the former GSPR (now IPRA) regarding the obligation of the Tax Offices to send reports to the Authority; and b. the large number of reports originating from Credit Institutions and Payment Institutions for suspicions of tax evasion in application of par. 7 of article 68 of Law No. 4174/2013 introducing the obligation to verify customer income for supervised institutions on the basis of the tax return statement.

ML Cases (originating from the above reports and information)¹⁰⁴

Year	2014	2015	2016
Total number	6.288	5.530	3.834
Derivation			
Banks	4.963	2.085	1.099
Insurance companies	201	390	496
Securities	37	43	45
Foreign Institutions-F.I.U.	33	164	178
Bureaux de change & Money Remitters	57	12	11
Public organizations and services	929	2.786	1.958
Complaints by individuals and other types of reports	---	50	47

Table17- ML Cases (originating from the above reports and information

Cases sent to the Public Prosecutor following freezing orders & corresponding criminal proceeds

Year	2014	2015	2016
Cases sent to public prosecutor	117	402	444
Freezed Assets (tax evasion, drugs, criminal organization, etc)	€160.937.720	€255.368.389	€301.740.646

Table18- Cases sent to the Public Prosecutor following freezing orders & corresponding criminal proceeds

The Authority exchanges confidential information with the respective prosecutorial or other authorities and services entrusted with investigatory, auditing or supervisory competences for the purpose of exchanging information or taking any further actions. The reception of feedback to the Authority is considered a critical issue, nevertheless, certain omissions have been noticed.

Cases for investigation - action - information

Cases forwarded for information, investigative and audit reasons	2014	2015	2016
Public Revenue Independent Authority	651	324	526
Gaming Commission	-	-	78
Hellenic Police	4	1	11
Financial Crime Investigations Unit	28	-	159
Other Ministerial Audit Agencies	4	-	14
TOTAL	686	325	788

Table19- Cases for investigation - action - information

¹⁰⁴Βλ. Έκθεση Πεπραγμένων Α' Μονάδας Διερεύνησης Χρηματοοικονομικών Πληροφοριών, έτους 2016.

The Authority is an active member both of the Egmont Group (since 1998) and of the European intelligence exchange network FIU.net since its establishment, while it has been effectively exchanging, upon request and/or spontaneously, financial or other types of information.¹⁰⁵

It is highlighted that up to 2016, seventeen (17) Memoranda of Understanding (MoUs) have been duly signed with foreign counterparts.¹⁰⁶ Finally, within the context of information exchange and by collaborating with competent domestic and foreign Law Enforcement Authorities (LEAs), including the National Europol and Interpol Offices, the Customs, and the Coastguard, the Authority is able to collect raw data related to cross-border activities.¹⁰⁷

3.5.5. Capacity and resources for financial crime investigations (including asset forfeiture)

Assessment rating: Medium High (0.6)

ML/TF investigations and the related predicate offences, apart from the Authority, are carried out by the Special Secretariat of the Financial and Economic Crime Unit, the Hellenic Police and the services of the Independent Authority for Public Revenue (IAPR)¹⁰⁸. The Financial Crime Investigations Directorate (FCID)¹⁰⁹ was recently established, which reports directly to the Minister of Finance, with the supervision and coordination of the Financial Prosecutor.

The Independent Authority for Public Revenue (IAPR), Special Secretariat of the Financial and Economic Crime Unit, Financial Police Directorate¹¹⁰ and Financial Crime Investigations Directorate (FCID), in the framework of their competences, have access to all the financial, tax and banking information of the investigated natural and legal entities without obligation to notify them, with the purpose of detecting any crimes committed and identifying assets. An important tool in financial investigations and the effective identification of assets is the Bank and Payment Accounts and Registries System¹¹¹, which despite certain technical deficiencies, provides access to bank account balances and bank transactions within 24 and 48 hours respectively.

In the context of the investigations and audits, the auditing and prosecution authorities identify the assets of the audited entities when their recovery is deemed necessary. Part of the Special Secretariat of the Financial and Economic Crime Unit, is the Hellenic Asset Recovery Office, which collaborates with its counterparts in the Member States of the European Union in order to trace and identify proceeds and other assets originating from cross-border criminal activities and which may be the subject of legal assistance for their freezing, seizure or confiscation in criminal cases.

The broad range of competences of the involved services, the overlap of their competences and/or lack of direct access to databases demonstrate a difficulty in the investigation of ML/TF cases and cause difficulties in the optimum use of human resources.

¹⁰⁵See Variable 1.3.15 «Effectiveness of International Cooperation».

¹⁰⁶Annex: Memorandum of Understanding (MoUs) by the AML/TF Authority.

¹⁰⁷The 1st Unit of the Authority, in the context of an effective collaboration, receives from the competent customs authorities an electronic file every quarter with all cash declarations, as submitted to the locally competent customs offices, and immediately those cases that require immediate action. The 1st Unit of the Authority keeps an electronic database (its data directly related to the STR database), and proceeds with prioritising and carrying out targeted audits based on criteria that have been set (amount of declared funds, frequency, country of origin, etc.).

¹⁰⁸See Annex "Financial Crime Investigation Services".

¹⁰⁹ Law 4512/2018, subchapter A (Article 381-390).

¹¹⁰ Separate Central Service of the Hellenic Police

¹¹¹Law 4170/2013 Article 62 .

Due to the increased demands for the conduct of financial investigations, the number of investigators in the competent services is not sufficient, but special emphasis is placed both on their education and their further education through training activities and seminars held in Greece and abroad.

3.5.6. Capacity and resources for financial crime prosecutors (including Asset forfeiture)

3.5.7. Capacity and resources for judicial processes (including asset forfeiture)

Assessment rating: Medium (0.5)

Assessment rating: Medium Low (0.4)

Judicial authority in Greece based on the Constitution consists of judges and prosecutors, without a clear distinction of judges and prosecutors who work exclusively on ML cases.

To address more specialised forms of crime, the institutions of Financial Crime Prosecutor¹¹² and Corruption Prosecutor¹¹³ were created. Moreover, at the Public Prosecutor's Office of the Athens Court of First Instance¹¹⁴, there have been appointed a) a competent public prosecutor who handles the case files submitted by the Special Secretariat of Financial and Economic Crime Unit. b) a special prosecutor responsible for cases concerning tax violations and c) specialised prosecutors at the preliminary investigation office handling cases related to financial crimes. When prosecutors conduct an investigation they have access to confidential information as provided for by general and special laws¹¹⁵. In the framework of the exercise of their duties, they may consult with specialised scientists or experts on the subject of their investigation^{116,117}

According to the Courts Regulation Code¹¹⁸ there is no provision for specialised judges or courts in relation to financial crimes or ML and the relevant cases are tried by criminal court judges, without distinguishing between crime categories.

Judges and prosecutors are appointed following a public competition and training at the National School of Judges. The training has a theoretical and a practical part and lasts 16-18 months. Then, their scientific background is judged by a Special Review Board¹¹⁹ on an annual basis and a reasoned assessment is drawn up¹²⁰. The training of judges and public prosecutors during their careers is ongoing through the National School of Judges. More specific subjects on financial crime and ML/TF are taught in the framework of a general course on special criminal laws, and seminars are organised to update their knowledge, which are not however integrated in a uniform and periodic training programme.

As regards the budget of prosecution and judicial authorities, allocations are not distinguished on the basis of the crimes prosecuted, nor is there any funding of specific branches of justice. However, we see an increase in allocations in the overall expenditure of the state budget during years 2014-2016. As regards the state expenditure restraint imposed by the financial circumstances, the above increases demonstrate the will to reinforce Justice award mechanisms.

¹¹² Law 2523/1997 Article 17A.

¹¹³ Law 4170/2013 Article 76 .

¹¹⁴ Document No. 196526/2017 of the Director of the Prosecutor's Office of the Athens Court of First Instance.

¹¹⁵ Law 2523/2017 article 17A para. 8 on the Financial crime prosecutor, Law 4205/2013 on the Corruption prosecutor and Law 3691/2008 Article 50 that applies in general for preliminary examination cases by all the Prosecutors.

¹¹⁶ Law 2523/1997 article 17A para. 9 and 10 of Law 4022/2011 article 2 para. 3.

¹¹⁷ With Law 4472/2017 which amends the relevant provisions of Article 17A of Law 2523/1997 a specialised service is created with special scientific staff for the investigation of tax evasion and other financial crimes.

¹¹⁸ Law 1756/1988.

¹¹⁹ Constitution Article 87 para. 3 and Law 1756/1988 Articles 80 et. seq.

¹²⁰ Law 1756/1988 Article 85.

Year	Judges	Prosecutors
2014	1693	559
2015	1732	572
2016	1752	580

Table 20 – Number of Judges and Prosecutors 2014-2016

An increase of the number of judges and prosecutors, but also of the investigated cases, regarding ML and predicate offences, can be observed during 2014-2016.

3.5.8. Integrity and independence of financial investigators (including Asset Forfeiture)

Assessment rating: Medium High (0.6)

The integrity and independence of financial investigators/auditors is protected when they are acting within the legal framework of their competences. Civil servants are covered by the Code of Civil Servants,¹²¹ whereas police officers by the disciplinary law and regulations of the police.¹²²

Also, with the purpose of ensuring common principles and codes of conduct for the employees of the Ministry of Finance and the Independent Authority for Public Revenue, there is a Code of Ethics and Conduct in place. Auditors are persons required to submit a Statement of Assets and a Statement of Financial Interests¹²³, as applicable, to the 3rd Unit of the Authority, to the General Inspector of Public Administration, to the Hellenic Police Internal Affairs Division and to the Independent Authority for Public Revenue. The employees of the Ministry of Finance and the Independent Authority for Public Revenue, and the Special Duties Officers of the Hellenic Police are recruited through tender notices that are carried out and supervised by the Supreme Council for Civil Personnel Selection (ASEP), a fact that ensures transparency in the method of their recruitment, whereas police officers enter the Force mainly through entrance examinations.

Money laundering investigations are conducted either in the framework of a public prosecutor's order following the investigation of a predicate offence, where responsible for evaluating the evidence is a public prosecutor, either following a complaint or an investigation, where responsible is the appropriate service each time in the framework of its operation. Law enforcement authorities and agencies operate on the basis of action parameters that aim at the transparency and objectivity of the audits, using planning criteria and means, such as risk analysis methods, data available from databases, cross-checking, statistical analysis and other sources of information¹²⁴. The employees of these services have access and obtain any information or data concerning or related to the performance of their work and their mission, following an official order, not being subject to restrictions of confidentiality provisions.

¹²¹Law 3528/2007 "Ratification of the Staff Regulations of Public, Political, Administrative Employees and Employees of Legal Persons governed by Public Law".

¹²² Presidential Decree 120/2008 "Disciplinary Law of Police Staff" and Presidential Decree 254/2004 "Police Officers' Code of Conduct". See also Annual Reports of Hellenic Police Internal Affairs Division, Ministry of Finance, Independent Authority for Public Revenue.

¹²³Law 3213 (Government Gazette Issue A 309/31.12.2003), as in force "Declaration and Audit of Assets of Public Officials, Media Owners, and Other Individuals".

¹²⁴ Annual Report of Coordinating Body of Inspection and Audit (SOEE) for year 2016.

3.5.9. Integrity and independence of financial crime prosecutors (including Asset Forfeiture)

3.5.10. Integrity and independence of judges(including Asset Forfeiture)

Assessment rating: High (0.7)

Assessment rating: High (0.7)

According to the fundamental principles of the Constitution, the judiciary in Greece is governed by the principle of independence.¹²⁵

The integrity of prosecutors and judges, is reinforced by the procedures of their recruitment, placement, transfer, promotion and evaluation, which serve as safeguards for their transparency.¹²⁶ Matters of disciplinary control of the judiciary are regulated in detail in the relevant laws¹²⁷, which provide for specific disciplinary instruments which are comprised of higher or supreme members of the judiciary without the intervention of the executive. Also, the law¹²⁸ refers to specific rules of exclusion and/or exemptions of prosecutors and judges from the assignment and handling of cases where there are suspicions of bias.

Moreover, actions are taken to ensure that the procedural rules offer further guarantees against delays in the judicial processes, the issue of a code of professional conduct and integrity standards for judges and prosecutors, as well as the achievement of further development and implementation of the ongoing training of judges and prosecutors on subjects of integrity. The issue of a number of court rulings is pending, a fact arising both from the high number of cases, and the complexity of the law. Also, the lack of a uniform information system and the general computerised support of the judicial and prosecution authorities leads to an inability by stakeholders to follow up, stay informed and keep reliable statistics.¹²⁹

In certain cases alone can the Minister of Justice ask the supreme prosecution officers to conduct a preliminary investigation or bring the case to a hearing in absolute priority¹³⁰. It has not yet been deemed necessary to use this option¹³¹. When political persons are involved in cases, competent to initiate a criminal prosecution is the Parliament for Ministers, whereas in the cases of members of parliament their immunity must be waived by the Parliament and the criminal prosecution conducted by the judiciary.¹³²

Important cases have been investigated, prosecuted and tried, mainly for corruption related to political persons and in general persons with a significant economic, social and political influence, with the corresponding asset recovery procedures provided for in each case.¹³³

¹²⁵ Constitution of Greece Article 87.

¹²⁶ Law 1756/1988 "Code on the Organisation of Courts and Status of Judicial Officers"

¹²⁷ Law 1756/1988 "Code on the Organisation of Courts and Status of Judicial Officers"

¹²⁸ Criminal Procedure Code Articles 14, 15 and 23 and Law 1756/1988 Article 8

¹²⁹ GRECO: Evaluation Report - 4th Evaluation Round: Corruption prevention in respect of members of parliament, judges and prosecutors

¹³⁰ Code of Criminal Procedure Article 30 para.3 of

¹³¹ GRECO: Evaluation Report - 4th Evaluation Round: Corruption prevention in respect of members of parliament, judges and prosecutors

¹³² Constitution of Greece Article 62

¹³³ See case of corruption (passive corruption) and money laundering with involvement, *inter alia*, of a political person (former Minister): Judgement No. 2384, 2471, 2474, 2531,2532, 2754, 2892, 2893, 2961, 3298, 3582, 3827, 3932, 3960, 3961, 3986, 4097, 4129, 4130, 4132, 4137 and 4554/2013 of first instance of the 3rd Three-member Court of Appeal of Felonies, where among other things, a large number of movable and immovable assets were confiscated.

3.5.11. Quality of border controls

Assessment rating: Medium (0.5)

Greece's geomorphological features are particular, with an extensive shoreline of about 15,000 kilometres, numerous islands and rock islets, a large number of airports and ports, and a strategic position between three continents. These elements render it a region of special interest and action for international organised crime networks, especially as a transit country for the further forwarding of proceeds of crime and irregular immigrants to the rest of the EU.

Despite not having clear indications and confirmed seizures, the numerous passages can be used in the smuggling of valuable stones, metals and cash¹³⁴. Control of the external borders of Greece and the EU is regulated by the Schengen Borders Code. The competent services are the Hellenic Police, the Hellenic Coast Guard and the Customs Authorities. More specifically:

- The Hellenic Police is responsible for passport control, through the legislated points of entry into the country (terrestrial, marine, air), implementing the provisions of the Schengen Borders Code (EU Regulation 2016/399), the surveillance of external borders, the receipt and identification of third-country nationals who enter illegally and reside in the country, their repatriation and combating in general any form of organised cross-border crime.
- The Coast Guard is responsible for imposing the law on ships, the sea and the ports, for the surveillance of the external borders and for combating any form of organised cross-border crime.
- Customs Authorities are responsible for conducting customs checks at the country's established points of entry-exit in accordance with the provisions of the national customs code.

The central databases used are: a) the national databases, b) the Schengen information system (SIS II), c) the information system for VISAs (VIS), d) the European fingerprint system comparison system (EURODAC), e) the Interpol database, f) the integrated customs system (Icisnet), g) the IAPR information system (Elenxis) and h) the European system of information exchange between customs authorities (AFIS).

For a comprehensive border management, Greece has established the National Coordination Center for Border Control, Immigration and Asylum, its competences including, inter alia¹³⁵: a) the coordination of the operational cooperation between co-competent, at national level, bodies and agencies, b) the coordination and monitoring of actions and measures implemented in the context of the national and European policy in the areas of border control, immigration and asylum and c) the collection of information and statistics from all co-competent bodies, in order to address irregular immigration.¹³⁶ As regards the established entry and exist check-points, which do not coincide precisely with the general meaning of "borders"¹³⁷, the customs authority carries out strict checks (of travellers, vehicles, undeclared cash, fuel, drugs and counterfeit products), supported by the Mobile Inspection Teams¹³⁸.

¹³⁴See Chapter "Threats", where the major threats identified, among others, are irregular immigration and drug trafficking.

¹³⁵Article 27 of Law 4058/2012, as amended and in force.

¹³⁶The Hellenic Police, with the "ASPIDA" operation at the Evros region, has managed to restrict the phenomenon of irregular immigration through the Greek-Turkish borders, thus leading to the discovery of other transit routes into the EU (land Bulgarian-Turkish borders and sea Greek-Turkish borders).

¹³⁷Points of entry-exit, other than certain land checkpoints, are also airports and ports.

¹³⁸The Mobile Inspection Teams are based at various Customs offices, and have as their purpose the conduct of preventive and ex-post customs inspections for the enforcement of customs and relevant tax laws, the prosecution of customs evasion and smuggling, the illicit trafficking of products and prohibited goods, as well as violations of any other laws, whose implementation has been assigned to the customs authorities.

Indicatively, the main violations identified during the 2014-2016 three-year period, in fifteen (15) selected border customs offices relate to counterfeit products, cash, tobacco products, oil and passenger exemptions.

Data from inspections carried out by the customs authorities during 2015 are presented below:

S/N	CONTROL CATEGORY	TOTAL CONTROLS	TOTAL INFRINGEMENTS
1	VAT exemption of imported goods destined to another EU Member State. (procedure 42)	98	12
2	Controls of duty-free shops	265	4
3	Couriers	401	23
4	Counterfeit goods	4,003	302
5	Control of cash on departure	8,236	91
6	Control of cash on arrival	6,016	76
7	Controls on alcohol trafficking	6,095	147
8	Controls on tobacco trafficking	6,584	169
9	Controls on petroleum product trafficking	3,274	40
10	Controls on the legitimate possession and movement of vehicles	5,575	777
11	Controls on ship supplies of fuels and other supplies	2,959	52
12	Controls on legal use of oil	1,171	27
13	Passenger reliefs from customs duty	10,343	1,016
14	Controls of fuel quantity of private truck tanks coming from third countries	1,455	201
15	Controls under T.984/79/A0019/2004	8,997	370
16	Controls for drugs	8,207	36
TOTAL		73,679	3,343

Table 21- Controls performed in the year 2015

3.5.12. Comprehensiveness of customs regime on cash and similar instruments

Assessment rating: Very High (0.8)

Inspections for cash in Greece are mainly based on Regulation 1889/2005 on the control of cash coming into or exiting the Community, and according to which a person entering or exiting the Community and carrying cash of a value equal to or greater than 10,000 euros must declare this amount to the competent authorities of the Member States. Competent authorities in our country are the customs authorities

(based on Article 3§2α v.2960/2001 of the national customs code and Ministerial Decision E2320/976/A0034/10.6.2008, Gov. Gazette, Series II 1177). Cash includes apart from cash, also negotiable bearer securities (cheques, bills of exchange, payment orders, etc.). Valuable metals and stones are not included, but failure to declare gold or valuable stones during entry from and into a third country may cause enforcement of the provisions on smuggling.

According to article 147(8) of Law 2960/2001 failure to declare cash is subject to a fine amounting to 25% of the cash found¹³⁹, whereas the above MD provides that the Customs Office that identifies the non-declare cash may seize the total amount found and send the case for further investigation to the Authority. If a link is found between the cash and illegal activities, the case is referred by the Authority to the competent prosecution authority, otherwise the amount remaining after deducting the fine is returned to the person that was carrying it.

At this time, a revision of the Regulation is under way, and the new texts being drawn up include gold and a possibility of seizing amounts under the €10,000 if there are indications that they are linked to illegal activities.¹⁴⁰

It is noted that in Article 4 of the Legislative Act No. 18/2015 (OGG A 84/2015) there is a provision that “the transport of banknotes in euro or foreign currency up to the amount of two thousand (2000) euros or the equivalent in foreign currency per natural person and per trip abroad is specifically allowed, until the issue of the Act of the Governor of the Bank of Greece provided for in paragraph 17 of this Article”.

3.5.13. Effectiveness of customs controls on cash and similar instruments

*Assessment rating: Medium (0.5)*¹⁴¹

The situation in cash inspection for the years 2014-2016 can be depicted by the following table:

YEAR	STATEMENTS SUBMITTED	AMOUNTS OF STATEMENTS SUBMITTED	INFRINGEMENTS NON DECLARATION OF LIQUID ASSETS	NON-DECLARED AMOUNTS OF LIQUID ASSETS	FINES IMPOSED
2014	4.168	145.073.780,70	149	7.058.992,98	1.811.766,21
2015	4.478	156.465.950,00	168	5.188.382,53	1.330.226,43
2016	4.413	132.396.059	212	7.551.230,17	1.933.008,79

Table 22- Liquid asset controls 2014-2016

¹³⁹Law 2960/2001 (National Customs Code), Article 147 para., 8.

¹⁴⁰ COM(2016) 825 Final, Brussels 21-12-2016, Proposal for a Regulation of the European Parliament and of the Council on controls on cash entering or leaving the Union and repealing Regulation (EC) No 1889/2005.

¹⁴¹ During 2014-2016, the Directorate-General for Customs and Excise Duty has taken various measures and initiatives to improve the efficiency of the Country, which shall be evaluated in the next update of the NRA, such as:

a) The ISEC participated in all the European fora overseeing the implementation of Regulation 1889/2005, while it submits questions related to the correct application of the Regulation or practical problems that arise. b) - The number cash-sniffing dogs is now 5, while there is a plan for the acquisition and training of new dogs in 2019, c) Posters have been posted to all exit point customs offices d) The Customs Service participated in at least 5 operations during the three-year period 2014-16 relating to the detection of cash (2016 212 cases and 2017 261 cases), e) The liquid assets chapter is part of the material to be taught by the Taxation and Customs Academy with specialist trainers from the Central Office. And f) If the methods of concealed cash are of particular interest, all the customs offices concerned are informed accordingly.

During the above years (2014-2016), 90% of the ascertained violations were recorded in three (3) customs offices (Athens Airport, Kipi and Evzonoi). This imbalance is probably due, in addition to the high passenger traffic, also to the understaffing of customs offices and the irrational allocation of the staff. The constantly increasing official requirements, as well as the fact that the greatest percentage of the country's customs (65 in a total of 91) are entry-exit points checking passenger traffic at land borders, airports and ports, result in a need to intensify inspections by reinforcing them with human and material resources.

Citizens are informed about the law on cash mainly at the local customs offices, with posters in various languages.

Customs Offices were recently reinforced with three cash detection dogs (Athens Airport, Evzonoi and Kipi), one for both cash and tobacco products (covering inspection needs both in the 1st Customs Office of Thessaloniki and the Thessaloniki Airport), and one that detects both cash and narcotic substances (Kipoi Customs Office). There are also thirteen (13) fixed baggage and parcel X-Ray scanners, one (1) mobile X-RAY baggage and package scanner and five (5) mobile systems for the inspection of trucks and containers with X-rays.¹⁴²

There is no risk analysis system in place, and it would be useful to combine its creation with the receipt of data from the Passenger Data Unit, by virtue of the incorporation of Directive 2016/681/EC on passenger name records (PNR)¹⁴³.

3.5.14. Effectiveness of domestic cooperation

Assessment rating: Medium High (0.6)

All law enforcement authorities and agencies (judicial, prosecution, auditing, law enforcement, supervisory authorities), collaborate on ML/TF issues with each other and mainly with the Authority¹⁴⁴. To support inter-service collaboration and achieve the best coordination, the following agencies have been created:

- the Supervision and Coordination Organisation Body¹⁴⁵ (SOEE), with the purpose of monitoring and coordinating the involved bodies and carrying out joint inspections and audits, especially in cases of corruption in the public sector.
- the Coordinating Operational Center¹⁴⁶, (COC) for addressing the smuggling of products subject to excise tax, which is supervised by the Operational Planning committee created by a decision of the Prime Minister.¹⁴⁷
- the Central Anti-Drug Coordinative Unit/National Intelligence Unit (CADCU-NIU)¹⁴⁸, which also functions as a National Information Unit for drugs.¹⁴⁹ The CADCU-NIU's creation was dictated in view of

¹⁴² To reinforce the effectiveness of customs inspections, the supply of twenty three (23) more package scanners, eight (8) mobile X-ray scanners, two (2) Gantry type and two (2) X-RAY scanners for trains were included in a NSRF programme.

¹⁴³The bill for the incorporation of Directive 2016/681/EC on passenger name records (PNR) has already been published, and the public consultation has also been completed.

¹⁴⁴See Variable 1.3.4 "Quality of FIU Intelligence Gathering and Processing".

¹⁴⁵SOEE: Law 3074/2002

¹⁴⁶SEK: Law 4410/2016 Article 6.

¹⁴⁷The President of the SEK is an employee of the General Directorate of Customs and Excise Tax of the Independent Authority for Public Revenue (IAPR), whereas its vice-president will come from the Hellenic Police. Employees from the General Secretariat for the Fight Against Corruption, the Internal Affairs Division, the IAPR, the Coast Guard, the Special Sectoral Secretariat for the Financial and Economic Crime Unit and the Coordination Center against Illegal Trade (SYKAP).

¹⁴⁸SODN: P. D. 139/1989 and 126/1990.

the effort to harmonise with EU directives for the establishment of such units in all Member States, with ultimate goal the uniform manner in addressing the problem and the assurance of a better system for the exchange and use of information.

- the Coordinating Center of Market Supervision and Addressing Illegal Trade¹⁵⁰ (ΣΥ.Κ.Ε.Α.Α.Π.), with participation of representatives of all national prosecution authorities with the aim of operational coordination in the illegal trade sector

Moreover, the General Secretariat for the Fight Against Corruption plays a critical role in the national cooperation¹⁵¹, since it is an institutional coordinating agency, with powers of supervision and initiative at a political and legislative level for all control mechanisms, structures and services responsible to fight corruption. It cooperates with international organisations, instruments and services of the EU or other states, and it has been defined as the authority responsible for coordinating the fight against fraud (AFCOS). A national strategic plan has been drawn up through the GSAC¹⁵² to address in an organised and targeted manner the multifaceted phenomenon of corruption.

The action of the supervisory authorities (BoG, Hellenic Capital Market Commission, Independent Authority for Public Revenue, etc.) enables the effective cooperation on ML/TF subjects also with the private sector, aiming at an exchange of information, know-how and ML recognition methods. The supervised bodies are required to forward data to prosecution and preliminary investigation authorities, as appropriate in accordance with the applicable laws.¹⁵³

3.5.15. Effectiveness of international cooperation

Assessment rating: High (0.7)

Greece has a complete legislative framework in place to ensure an effective international and European cooperation, both at judicial/prosecution and at operational level, having ratified and implemented the majority of the European and international legislative texts, the last being the ratification and adaptation of the Greek laws to the Warsaw Convention¹⁵⁴, as well as the incorporation of Directive 2014/41/EU regarding the European Investigation Order in criminal cases¹⁵⁵.

The Ministry of Justice, Transparency and Human Rights operates as a central authority for international cooperation at level of judicial and prosecution authorities. This cooperation pertains initially to the provisions of judicial assistance between the judicial and prosecution authorities of both sides, as well as the extradition of requested persons. Greece's systematic participation in the European Judicial Network¹⁵⁶ and the Judicial Cooperation Unit of the EU (Eurojust)¹⁵⁷, decisively reinforce the effectiveness in the investigation and prosecution of serious crime.

¹⁴⁹ Members and their substitutes come from the competent Prosecution Authorities (Hellenic Police, Customs Service, Coast Guard and Special Audit Service) and are appointed by the co-competent Ministers with a two-year term. Its president is a representative of the Hellenic Police.

¹⁵⁰ SYKEAAP: Law 4155/2013

¹⁵¹ It was established with Law 4320/2015 (Government Gazette A'29), which sets out the institutional framework of its operation and it is subject to the Deputy Ministry of Justice, Transparency and Human Rights.

¹⁵² See website of General Secretariat against Corruption (GSAC). http://www.gsac.gov.gr/attachments/article/122/GR_National%20Anticorruption%20Plan_31_12_2016.pdf

¹⁵³ The Bank of Greece has provided information after waiving the banking confidentiality to Prosecution authorities and supervised financial institutions for 558 cases during the past three years, and to the Financial Police Division for 99 cases.

¹⁵⁴ Law No 4478/17 (Gov. Gazette Series I, 91/23.06.2017)

¹⁵⁵ Law No 4489/17 (Gov. Gazette Series I, issue 140 21.9.2017)

¹⁵⁶ On the basis of Article K3 para. 2 of the Treaty on European Union, Council Joint Action 98/427/JHA of 29 June 1998 by the Council established a European Network of judicial associations. The Ministry of Justice, Transparency and Human Right has defined as contact persons judges and prosecutors of the Courts of Appeal of Athens, Piraeus and Thessaloniki, two court employees of the Prosecutor's

Extraditions and European Warrant Arrests ¹⁵⁸

BY FOREIGN AUTHORITIES		
YEAR	REQUESTS	EXECUTIONS
2014	66	52
2015	69	55
2016	81	50
BY GREECE		
YEAR	REQUESTS	EXECUTIONS
2014	14	4
2015	16	3
2016	8	1
EUROPEAN WARRANT ARREST BY GREEK AUTHORITIES		
YEAR	REQUESTS	EXECUTIONS
2014	269	165
2015	227	161
2016	312	149

Table 23- Extraditions and European warrant arrests

Also, the Ministry of Justice, Transparency and Human Rights actively participates in working groups of the European Council, the United Nations (UN) and the Organisation for Economic Co-operation and Development (OECD), as well as other regional organisations¹⁵⁹. International judicial cooperation in criminal cases is based on intra-national bilateral or multilateral agreements¹⁶⁰.

Judicial Assistance Requests (Prosecutor's Office of Athens Court of Appeal)¹⁶¹

YEAR	TOTAL REQUESTS	INCOMING	OUTGOING	TOTAL CASES
	FOR JUDICIAL ASSISTANCE			(ML/TF, Corruption, Economic Crimes)
2014	704	19	141	160
2015	651	18	69	87
2016	681	49	86	135
TOTAL	2036	86	296	982

Table 24- Judicial assistance requests (Prosecutor's Office of Athens Court of Appeal)

Moreover, in Greek legal order, Law 3663/2008 (Government Gazette A 99/2008)¹⁶² as amended and in force¹⁶³ provides for the establishment of common investigation teams for ascertaining serious crime.

Office of the Athens Court of Appeal as well as two employees of the Central Service of the Ministry of Justice, Transparency and Human Rights.

¹⁵⁷ Eurojust was created with Decision 2002/187/JHA of the Council, as amended with Decision 2009/426/JHA of the Council, of 16 December 2008. A Deputy Prosecutor of the Court of First Instance has been appointed representative of our country at Eurojust. See relevant webpage <http://www.eurojust.europa.eu/Pages/languages/el.aspx>

¹⁵⁸ Statistics by Ministry of Justice, Transparency and Human Rights

¹⁵⁹ See Website of the Ministry of Justice, Transparency and Human Rights <http://www.ministryofjustice.gr/site/el/>

¹⁶⁰ See Website of the Ministry of Justice, Transparency and Human Rights <http://www.ministryofjustice.gr/site/el/>

¹⁶¹ Statistics by the Athens Court of Appeal Prosecutor. The Athens Court of Appeal Prosecutor receives, dispatches and handles about 80% of the total number of judicial assistance requests

¹⁶² The Council framework decision 2002/465/JHA was incorporated

Also, according to article 19 of Law 3875/2010, the Member States in the UN Convention against International Organised Crime aim at the conclusion of bilateral or multilateral agreements or arrangements, based on which the interested competent authorities may establish common investigation instruments, for cases that are the subject of investigation, prosecution or court procedures in one or more countries. If there are no such agreements or arrangements, joint investigations may be decided as appropriate.

In the context of the judicial cooperation in criminal cases and cases of extradition of criminals, the channel of the International Police Cooperation Division of the Hellenic Police Headquarters is used especially in urgent cases.¹⁶⁴

At operational level, international cooperation is achieved through law enforcement authorities and bodies, and the security of the information is assured with security protocols and classification codes, and in particular:

The international collaboration of the Hellenic Police and the other law enforcement authorities takes place through the established communication channels of EUROPOL, INTERPOL and SIRENE¹⁶⁵, through special information exchange platforms, and it is deemed to be fast and effective.

Within the Central Agency of Financial and Economic Crime Unit is operating the National Asset Recovery Office for funds and assets deriving from criminal activity (Hellenic Asset Recovery Office - ARO Greece), which cooperates with the corresponding departments of the EU member states to detect, and trace, proceeds and other assets deriving from cross border criminal activities and which may be the subject of legal assistance for freezing, seizure or confiscation in criminal cases. Furthermore, Greece is a member of the CARIN network¹⁶⁶, of which ARO Greece is an active contact point. Moreover, there is a close collaboration between the Special Secretariat for Financial and Economic Crime Unit with EUROPOL, INTERPOL as well as the European Anti-fraud Office (OLAF)¹⁶⁷ supporting the immediate exchange of information in the fight against serious crime.

The Special Secretariat of Financial and Economic Crime Unit, and especially the A.R.O Greece, is connected to the Secure Information Exchange Network Application (SIENA) of EUROPOL, which serves the communication needs of the law enforcement authorities in the EU. Actions have also been taken for gaining access to the Europol Information System (EIS).

¹⁶³Article 62 of Law 4249/2014 (Gov. Gazette, Series I'73/24-03-2014). See also the very recent amendments caused by para. 10 of Article 24 of Law 4531/2018 (Government Gazette 62/A).

¹⁶⁴ Article 445 para.2 of the Code of Criminal Procedure and Article 16 para. 2 of Law 4165/61 "On the ratification of the European Convention on Extradition signed by Greece in Paris on 13 December 1957", Gov. Gazette 75/6-5-1961, Series I (Council of Europe) Article 15 of Law 4218/1961 "On the ratification of the European Convention on mutual judicial assistance in criminal cases", Gov. Gazette 171/19-9-1961, Series I (Council of Europe).

¹⁶⁵It is noted that the International Police Cooperation Division of the Hellenic Police Headquarters is also a channel for forwarding judicial assistance requests in urgent cases.

¹⁶⁶ The Camden CARIN network is an unofficial network of contact points and a collaboration group that engages in all aspects of the crime proceeds confiscation procedure. It is a network of professionals covering 54 different jurisdictions and 9 international organisations. It is connected to similar asset recovery networks in South Africa, Latin America, Asia-Pacific countries, East Africa and West Africa.

¹⁶⁷The AFCOS office of the General Secretariat for the fight Against Corruption is the coordinating service of the collaboration and exchange of information with OLAF.

Special Secretariat of Financial and Economic Crime Unit Information Exchange Requests between ARO – CARIN

YEAR 2016	Incoming requests	Outcoming requests	Investigations Natural persons	Investigations Legal persons
		27	13	120

Table 25- Information exchange requests through ARO-CARIN

Special Secretariat of Financial and Economic Crime Unit Incoming Information Requests EUROPOL-INTERPOL

Year	Total requests	
	EUROPOL	INTERPOL
2016	342	89
2015	242	19

Table 26- Special Secretariat of Financial and Economic Crime Unit (SDOE) Incoming information requests EUROPOL-INTERPOL

The Authority has been an active member of the Egmont Group since 1998¹⁶⁸, as well as of the FIU.net information exchange network¹⁶⁹, exchanging information with the corresponding Authorities of other countries. From 2012 to 2016, the Authority has signed nine (9) MoUs with counterparts abroad¹⁷⁰, reinforcing cooperation and exchange of information in fighting ML/TF. It also cooperates with the National Unit of Europol, Interpol and the corresponding services of third country Embassies.

Requests for Exchange of Information through FIU.net&Egmont Secure Web

	2014	2015	2016
Incoming requests	162	201	212
Outgoing requests	89	27	15

Table 27- Requests for exchange of information through FIU.net & Egmont Secure Web

The country's tax and customs authorities¹⁷¹ cooperate and exchange information with corresponding foreign services on the basis of relevant legislative texts and contracts¹⁷². The change of the information between EU Member States takes place through a special communication channel (CCN mail). We note

¹⁶⁸ The **EgmontGroup** organisation is a united body of 155 Financial Intelligence Units (FIUs) from across the world and aims to support and improve the understanding of ML/TF risks amongst its stakeholders, while supporting and promoting the cooperation and proper exchange of information between FIUs internationally. It provides the **EgmontSecure** platform for the secure exchange of expertise and financial intelligence to combat money laundering and terrorist financing (ML/TF). See <https://egmontgroup.org/content/about>

¹⁶⁹ Following the publication of decision 2000/642/JHA of 17 October 2000, by the European Council, the European Commission created the **FIU.net** electronic network for the connection of the EU Financial Information Units for the exchange of information between them. The FIU. net is a decentralised and advanced IT network that supports the Financial Information Units (FIUs) of the Member States in the European Union to fight money laundering and terrorism financing. The FIU.NET has been designed as an **exceptional secure channel of communication** for the exchange of information between the FIUs of the EU, whereas since 2016 it has been included in Europol. See <https://www.europol.europa.eu/about-europol/financial-intelligence-units-fiu-net>

¹⁷⁰See Annex "Memorandum of Understanding (MoUs)"

¹⁷¹ Independent Authority for Public Revenue (General Directorate of Tax Administration - General Directorate of Customs & Excise Taxes - Directorate of International Financial Relations)

¹⁷²Annex: Legislation and Agreements for International Cooperation

the recent Multilateral Competent Authority Agreement (MCAA) on the automatic exchange of financial account information exchange (Law 4428/2016, Gov. Gazette Series I 190/2016), that provides for information exchange based on Directive 2014/107/EU as well as the conclusion of fifty seven (57) Bilateral Double Taxation Avoidance Agreements¹⁷³.

Administrative Cooperation Information Exchange Requests IAPR

	2016
Incoming requests	39
Outgoing requests	167

Table 28- Administrative cooperation information exchange requests IAPR

Mutual Administrative Assistance in customs matters is defined as the general information exchange procedure between customs administrations with the purpose of preventing, detecting and suppressing violations of customs laws.

The Greek customs service engages in mutual assistance on a systematic basis with the competent services of both EU member states and third countries.

Between EU Member States, mutual assistance in customs matter is carried out:

- on the basis of Regulation 515/07 of 13 March 1997 on mutual assistance between the administrative authorities of the Member States and cooperation between the latter and the Commission to ensure the correct application of the law on customs and agricultural matters as amended by Regulation 766/2008 of the European Parliament and the Council of 9 July 2008 and Regulation 1525/2015 of the European Parliament and the Council of 9 September 2015.
- and on the basis of the Naples II Convention drawn up on 18 December 1997 based on Article K3 of the Treaty on European Union on mutual assistance and cooperation between customs services and ratified with Law 2772/1999 (Gov. Gazette Series I, 282/1999)

Between Greece and third countries (or certain EU member states that were third countries at the time these relevant agreements were entered into) mutual assistance on customs matters is conducted:

- on the one hand based on international bilateral agreements which Greece has concluded on a bilateral level and which have been ratified by the Hellenic Parliament according to Article 28 para. 1 of the Constitution
- on the other hand on the basis of international agreements which the European Union has entered into with a number of third countries, and which have either the legal form of a Protocol in international conventions of a broader content which the EU enters into with these third countries or the legal form of an independent international agreement.
- An additional exchange information possibility between customs administrations is provided based on the multilateral international convention for the creation of SELEC - Southeast European Law Enforcement Center (SELEC) which was ratified by Greece with Law 4054/2012 Gov. Gazette, Series I, 45 . The states-contracting members in the international SELEC agreement are the

¹⁷³See IAPR webpage http://www.gsis.gr/gsis/info/gsis_site/ddos/b.html

following: Greece, Bulgaria, Romania, Croatia, Hungary, Serbia, Albania, Bosnia-Herzegovina, FYROM, Moldavia and Montenegro.

The following table presents the statistical picture of incoming and outgoing assistance requests from and to the Greek Customs Service during the three previous years.

Requests of Exchange of Assistance Requests with EU Member States

YEAR	REQUESTS		ANSWERS	
	IN	OUT	IN	OUT
2014	21	34	17	8
2015	14	58	24	13
2016	20	67	40 (SATISFACTORY)	19
TOTAL	55	159	81	40

Table 29- - Requests of exchange of assistance requests with EU Member States

Requests of Exchange of Assistance Requests with third countries

YEAR	REQUESTS		ANSWERS	
	IN	OUT	IN	OUT
2014	75	77	47	45
2015	74	69	45	57
2016	111	89	83 (73 SATISFACTORY)	113
TOTAL	260	235	175	215

Table 30- Requests of Exchange of Assistance Requests with third countries

The supervisory authorities of Article 6 of Law 3691/2008 (Bank of Greece, Hellenic Capital Market Commission, Hellenic Gaming Commission, Hellenic Accounting and Auditing Standards Oversight Board) in the context of their competences based on European and international agreements participate in working groups and exchange information of an administrative nature with their counterpart authorities, through secure information exchange networks.

3.5.16. Availability of independent audit

Assessment rating: High (0.7)

Through the incorporation of the Hellenic Accounting and Auditing Standards Oversight Board (HAASOB - ELTE)¹⁷⁴, the supervising body for certified public accountants-auditors, and the amendments to the

¹⁷⁴ Law 3148/2003

legislative framework¹⁷⁵, issues concerning the statutory audits of annual accounts and consolidated accounts and the exercise of public oversight of audit work were regulated¹⁷⁶.

The ELTE grants approvals to certified public accountants-auditors or rejects the applications submitted by candidates, and sets the procedures, supporting documents and other details¹⁷⁷.

The reporting obligations of the regulatory compliance operations of audit firms are regulated every two years through internal notices. Furthermore, ELTE Regulatory Act 004/2009 regulates the obligations of certified public accountants-auditors concerning the prevention and suppression of ML/TF, while Notices 003/2012 and 002/2014 regulate the reporting obligations of the regulatory compliance operations of audit firms every two years.

The key audit partners responsible for carrying out a statutory audit under Article 16 of Regulation (EU) 537/2014 shall cease their participation in the statutory audit of the audited entity not later than five (5) years from the date of their appointment (Article 48 of Law 4449/2017).

Article 52 of Law 3691/2008 and ELTE Regulatory Act 4/2009 provide for administrative sanctions for failure to apply due diligence measures on the part of obligated parties.

Audit firms shall make public an annual transparency report¹⁷⁸ at the latest four months after the end of each financial year.

All public-interest entities shall have an audit committee consisting of at least three members. The audit committee shall be either an independent committee or a committee of the Board of Directors of the audited entity. Under Article 11 of Regulation 537/2014, certified public accountants-auditors or audit firms carrying out statutory audits of public-interest entities shall submit an additional report to the audit committee of the audited entity not later than the date of submission of the audit report explaining the results of the statutory audit and including, *inter alia*, their declaration of independence.

Under Article 10 of Law 3148/2003, as in force, the ELTE, the BoG, the Hellenic Capital Market Commission and the Ministry of Finance shall cooperate aiming at the effective exercise of their competencies. Each may forward to any other information or data useful for their work.

Under Law 4449/2017 the ELTE consults and cooperates with the professional association of certified public accountants-auditors for the issuance of regulatory acts and on auditing and accounting matters, and issues instructions and guidelines in the context of its communication with audit firms and certified public accountants-auditors.

Audit firms are obligated to maintain a system of quality safeguards¹⁷⁹ that shall include, *inter alia*, policies and procedures on issues concerning ethics and independence, as well as compliance of its staff

¹⁷⁵ Law 4449/2017, which replaced Law 3691/2008.

¹⁷⁶ Along with Regulation (EU) 537/2014, this envisages specific requirements regarding statutory audit of public-interest entities.

¹⁷⁷ Under Law 4449/2017, in order for certified public accountants-auditors to be granted an approval, the conditions set out in Articles 5 and 7 through 11 and/or 13 must be satisfied.

¹⁷⁸ This transparency report shall be published on the website of the audit firm and shall include, *inter alia*: i) revenues from the statutory audit of annual and consolidated financial statements of public-interest entities and entities belonging to a group of undertakings whose parent undertaking is a public-interest entity; ii) revenues from the statutory audit of annual and consolidated financial statements of other entities; iii) revenues from permitted non-audit services to entities that are audited by the statutory auditor or the audit firm; and iv) revenues from non-audit services to other entities. Additionally, each year audit firms shall submit a detailed list with the fees for audit and non-audit services to the ELTE.

¹⁷⁹ In accordance with the requirements specified in the International Standard on Quality Control 1 (ISQC-1),

with the code of ethics for professional accountants of the International Federation of Accountants (IFAC)¹⁸⁰.

Issues concerning the independence of certified public accountants-auditors and audit firms are regulated in Articles 20, 21, 25, and 26 of Law 4449/2017, whereunder certified public accountants-auditors or audit firms shall establish appropriate and effective organisational and administrative arrangements to prevent, identify, eliminate or manage and disclose any threats to their independence.

Under International Standard on Auditing 220, the responsible auditor is obligated to apply all the procedures necessary to ensure full compliance of the audit team with the relevant ethical and independence requirements. Finally, the obligated parties of Article 5 of Law 3691/2008 and, more specifically, banks, insurance firms and brokerage firms are subject to annual ordinary statutory audits by certified public accountants-auditors¹⁸¹.

3.5.17. Level of financial integrity

Assessment rating: Medium High (0.6)

Due to their complexity, financial crimes, fraud and corruption are becoming increasingly harder to identify and investigate, resulting in an adverse effect on the economy. Studies carried out during the last five years indicated that there is an increase in the number of occurrences of fraud, corruption and bribery in organisations and businesses, impeding Greek entrepreneurship and undermining the competitiveness of the economy.^{182,,183}

The Hellenic Corporate Governance Code for Listed Companies and the Special Practices of Good Corporate Governance for Non-Listed Companies are the key texts on corporate governance in Greece, as developed by the Hellenic Federation of Enterprises (SEV) and the Hellenic Corporate Governance Council (ESED). These are texts that have been adapted to Greek legislation and business reality, drafted on the basis of the “comply or explain” principle, thus including matters going beyond the laws and rules in force.

Additionally, codes of conduct have been drafted for numerous categories of professionals, such as accountants - tax consultants¹⁸⁴, attorneys¹⁸⁵, brokers, notaries public¹⁸⁶, and so forth. Under the legislative framework in force, there is an obligation to provide tax authorities with information on the income and property of entities active in Greece either as natural or as legal persons¹⁸⁷. The application of a mechanism as a tool for achieving good governance practices is of catalytic importance for the Greek economy, and this can only be achieved if the Hellenic Corporate Governance Code and the individual codes of conduct of the various bodies are incorporated into legislation and their application is mandatory. In 2005, the Greek Chapter of the European Business Ethnics Network (EBEN GR) was founded, aiming at disseminating knowledge and information on business ethics, corporate responsibility and governance.

¹⁸⁰IFAC: International Federation of Accountants.

¹⁸¹The audit criteria are set in Article 42a(6) of Codified Law 2190/1920.

¹⁸²World Economic Forum, Global Enabling Trade Report 2014 and Global Competitiveness Report 2016; US State Department, Investment Climate Statement 2015; Transparency International, National Integrity System Assessment Greece 2012.

¹⁸³Krambia-Kapardis, M. & Papastergiou, K. (2016). Fraud victimization in Greece: room for improvement in prevention and detection. *Journal of Financial Crime*, 23(2), 481-500.

¹⁸⁴Decision of the Deputy Minister of Development and Competitiveness No 57088/DIOE-1033/18.12.2013/ Gov. Gazette, Series II, 3314.

¹⁸⁵ Code of Lawyers under Law 4194/2013, Gov. Gazette, Series I, 208.

¹⁸⁶ Code of Notaries Public - Law 2830/2000, Gov. Gazette, Series I, 96.

¹⁸⁷Under Law 4172/2013 (Gov. Gazette, Series I, 167 23.7.2013) titled ‘Income Tax Code (KFE) (Articles 45, 67)’, Law 4223/2013 ‘Single Property Tax (ENFIA)’, Law 3213/2003 (Gov. Gazette, Series I, 309/31.12.2003) - Declarations of Assets and Declarations of Financial Interests; see also variable 1.3.18 ‘Effectiveness of Tax Enforcement’.

In order to improve transparency in Greece, under Law 3861/2010 ‘Enhancement of transparency through the obligatory uploading of laws and acts of governmental and administrative organs and organs of local government on the Internet’, all public bodies were obligated to upload their decisions, including those concerning public contracts, on the Internet (‘Diavgeia’ programme).

This information and data provided by the information systems of the Independent Authority for Public Revenue (IAPR), such as ‘MIS ELENXIS’, ‘ICISNET’, ‘TAXISNET’, ‘System of Bank Account and Payment Account Registries - SMTL&LP’, as well as the Application for the Automated Control of Asset Augmentation are contributing to the effectiveness of audits, both on a case-by-case and on an overall basis. The ELENXIS, ICISNET and TAXISNET Management Information Systems depict data provided by the persons in question to the competent authorities (tax returns, real estate property declarations, etc.) for the creation of their financial profiles. The operation of the System of Bank Account and Payment Account Registries (SMTL&LP)¹⁸⁸ is an important tool for carrying out audits, preventing unnecessary bureaucratic procedures and facilitating the work of auditors. Under the legislative framework in force, there is an obligation to provide tax authorities¹⁸⁹ with information on the income and property of entities active in Greece either as natural or as legal persons¹⁹⁰.

3.5.18. Effectiveness of tax enforcement

Assessment rating: Medium High (0.6)

In recent years, major reforms have been effected to tax legislation, aiming at simplifying tax procedures and addressing overregulation. More specifically, the Tax Procedure Code (KFD)¹⁹¹ was enacted in 2013; this was the first effort to concentrate and codify the procedures followed by tax services hitherto recorded in widely dispersed provisions. The issues it regulates includes the obtaining of information, the imposition of sanctions in cases of infringement of tax provisions and the safeguarding of taxpayers’ rights. This reform effort must remain ongoing for the overhaul of tax legislation and the modernisation of tax administration.

The authority competent for the enforcement of tax legislation is the Independent Authority for Public Revenue (IAPR), which was established on 01/01/2017¹⁹² and replaced the General Secretariat for Public Revenue in order to ensure the continuation and effectiveness of the tax administration and its independence from any type of political interference. The Authority enjoys functional independence, administrative and financial autonomy, and is subject to parliamentary scrutiny. Its mission is the assessment and collection of tax, customs and other public revenues within the scope of its remit, promoting tax compliance, combating tax evasion and smuggling, and providing high-quality services to citizens and businesses.

¹⁸⁸See Variable 1.3.6 ‘Integrity and Independence of Financial Crime Investigators’.

¹⁸⁹See Annex 21. Greek Agencies involved in Financial Crime Investigation.

¹⁹⁰Under Law 4172/2013 (Gov. Gazette, Series I, 167 23.7.2013) titled ‘Income Tax Code (KFE) (Articles 45, 67)’, Law 4223/2013 ‘Single Property Tax (ENFIA)’, Law 3213/2003 (Gov. Gazette, Series I, 309/31.12.2003) - Declarations of Assets and Declarations of Financial Interests; see also Variable 1.3.18 ‘Effectiveness of Tax Enforcement’.

¹⁹¹ Law 4174/2013.

¹⁹² Law 4389/2016.

In the context of its competencies, the IAPR may receive all the necessary information from taxpayers and third parties by using the methods envisaged in the Tax Procedure Code (KFD)¹⁹³. It may also exchange information with international services and bodies¹⁹⁴.

Tax compliance is achieved through a) actions undertaken by the Directorate of Tax Compliance b) with provisions concerning the voluntary disclosure of taxable items of previous years¹⁹⁵ and with audits in certain cases. There is also a set of provisions setting sanctions depending on the type of infringement (administrative and criminal sanctions for tax evasion offences). In any event, the tax administration imposes fines for administrative offences¹⁹⁶. In cases of tax evasion offences, criminal sanctions are imposed through a judgment issued by the criminal court seized of the case.

Tax audits of increased importance are carried out by special services¹⁹⁷ of the IAPR. Cases are audited as a matter of priority on the basis of risk analysis criteria, data from internal and external sources of information or, by way of exception, other criteria set by the Governor of the IAPR that are not made public. All audit steps are entered into the Elenxis computerised system, from the issuance of the audit order to the notification of the audit report and tax assessment, thus enhancing the transparency of the procedure.

Due to the increased requirements for combating tax evasion and collecting public revenues, as well as the considerable burden of prosecutorial orders, the number of auditors carrying out tax audits and tax collection is not sufficient. The employees of the IAPR attend training seminars on their field, while the Tax and Customs Academy ceased operating in 2017.

Additionally, the Financial Police Division (FPD) is competent to conduct tax audits; the Division drafts a special annual operational plan of actions used as a basis for conducted targeted tax audits following the processing of information.

Furthermore, by virtue of Law 4512/2017,¹⁹⁸ the Directorate of Financial Crime Investigation (DFCI) was established at the Ministry of Finance, reporting directly to the Minister of Finance. The Public Prosecutor for Economic Crime is tasked with guiding and coordinating the operation of the service. Its exclusive mission is to conduct investigations, preliminary examinations or preliminary investigations in order to ascertain the commission of crimes and any related economic crimes harmful to the interests of the Greek State and the European Union.

3.5.19. Formalization level of economy

Assessment rating: Medium (0.5)

The shadow economy or informal economy includes all undeclared economic activities that, despite producing added value, are not recorded in the official estimates of the gross domestic product (GDP). Although the shadow economy and tax evasion are not synonymous concepts, in most cases shadow economy activities entail the loss of indirect or direct taxes, leading to the loss of tax revenues. In fact, the possibility of tax evasion is a key incentive for the development of informal economy activities.

¹⁹³ Articles 14 and 15 of Law 4174/2013

¹⁹⁴ See Variable 1.3.15 'Effectiveness of International Cooperation'.

¹⁹⁵ Articles 57 through 60 of Law 4446/2016.

¹⁹⁶ See General Secretariat of Public Revenue (GGDE) Annual Report for the year 2016

¹⁹⁷ Audit Centre for Large Enterprises (K.E.ME.EP.), Audit Centre for High Wealth Individuals (K.E.F.O.ME.P), Services for Investigations & Safeguarding of Public Revenue (Y.E.D.D.E.)

¹⁹⁸ Gov. Gazette, Series I, 5-17.01.2018

Under Articles 39 and 40 of Law 4155/2013, illegal trading is defined as any movement or sale of merchandise in any way without the anticipated professional licence or the statutory receipts/invoices. Illegal trading falls within a broader circle of misconduct and at times coexists with other illicit activities, such as: concealment of taxable items, smuggling, infringement of intellectual property and trademark (imitation, falsification, pirating).

The size of the shadow economy in Greece is relatively high in comparison to other developed countries of the OECD. The shadow economy in Greece dropped to 23.6% of the GDP in 2013, as compared to 24% in 2012, 25.1% prior to the crisis of 2008 and 28.2% in 2003. In 2015, the shadow economy in Greece is nearly 22.4% of the GDP, almost one fourth of all economic activity, a high percentage among OECD countries¹⁹⁹. At present, illegal economic activities are estimated at just over 20% of the national income²⁰⁰, a drop caused by the extended economic crisis and relevant reforms. Greece holds a high position in the shadow economy level of the 27 EU Member States, considerably higher than the EU average²⁰¹. In 2016, the value of the Greek GDP represented 0.31% of the global economy²⁰².

Audit mechanisms and law enforcement bodies are intensifying their actions to combat these phenomena (illegal trading, undeclared work, protection of intellectual property, smuggling, etc.) in order to achieve an environment of healthy competition and consumer protection.

In cases of financial crimes of infringement of intangible assets, there are often issues of criminal sanctions regulated by the special part of the Penal Code - 'Documented-related criminal offences'²⁰³.

Law 4177/2013 and Ministerial Decision 91354 (Gov. Gazette, Series II, 2983/30-08-2017) regulate and codify the rules governing the movement and trading of products and the provision of services.

In order to combat illegal trading, the Coordination Centre for Market Oversight and Combating Illegal Trading (CCMOCIT/SYKEAAP)²⁰⁴ coordinates and cooperates with the competent authorities, concentrates and analyses information and data deriving from audits carried out by individual competent authorities.

The effective combating of illicit trade and the coordination of the services involved in combating smuggling are achieved through the Operations Coordination Centre (OCC/SEK).²⁰⁵

¹⁹⁹ On the methodology compare e.g. Feld and Schneider (2010), Schneider, Buehn and Montenegro (2010), Schneider and Enste (2000, 2006), Schneider (2005), and Dell'Anno and Schneider (2009).

²⁰⁰Institute for Applied Economic Research (IAW), University of Tübingen, Germany (2017)

²⁰¹Schneider (2013), Size and development of the Shadow Economy of 31 European and 5 other OECD countries from 2003 to 2013: a further decline, Johannes Kepler University, Linz.

²⁰²Retrievable in <https://tradingeconomics.com/National-Statistical-Service-of-Greece>

²⁰³Articles 216-223 of the Penal Code

²⁰⁴Article 100 of Law 4497/17. The SYKEAAP consists of: a. The Secretary General for Trade and Consumer Protection as Chairperson; b. The executive officer; c. A representative of the General Secretariat for Trade and Consumer Protection of the Ministry of Economy and Development; d. A representative of the Hellenic Police (E.A.); e. A representative of the Hellenic Coast Guard (L.S.); f. A representative of the Financial and Economic Crime Unit (SDOE); g. A representative of the General Directorate of Customs and Excise Duty of the Independent Authority for Public Revenue (IAPR); h. A representative of the Central Union of Municipalities of Greece (KEDE); i. A representative of the Association of Greek Regions (ENPE); j. A representative of the General Secretariat for Industry; k. A representative of the General Secretariat for Rural Development; l. A representative of the Directorate of Combined Transport of the Ministry of Infrastructure and Transport; m. A representative of the Union of Hellenic Chambers; n. A representative of the Hellenic Confederation of Commerce and Entrepreneurship (ESEE); o. A representative of the Hellenic Confederation of Professionals, Craftsmen & Merchants (GSEVEE).

²⁰⁵Article 6 of Law 4410/2016. By virtue of a decision issued by the Secretary-General for Public Revenue, the SEK consists of employees seconded for this purpose from the following services: a) One employee of the General Directorate of Customs and Excise Duty of IAPR as Chairperson; b) One employee of the Hellenic Police as Vice-Chairperson; c) One employee of the General Secretariat against Corruption as Secretary; d) One employee of the Directorate of Internal Affairs of the General Secretariat for Public Revenue as a member; e) One employee of the Hellenic Coast Guard as a member; f) One employee of the Special Secretariat of the Financial and Economic Crime Unit as a member; g) One employee of the General Secretariat for Trade - Coordination Centre Against Illicit Trade (SYKAP) as a member. The Operations Coordination Centre is staffed by twenty (20) employees seconded from the foregoing services.

In order to combat undeclared work, audits are carried out, with the use of mixed teams, by the Labour Inspectorate²⁰⁶ (LI/SEPE), the Regional Insurance Audit Centre²⁰⁷ (RIAC/PEKA) of the Unified Social Security Fund (EFKA), the Special Secretariat of the Financial and Economic Crime Unit (FECU/SDOE) and the Financial Police Division (FPD/DOA).

The contribution of the General Secretariat against Corruption with respect to coordination is also significant.

In the context of the above, joint operations are carried out with law enforcement authorities or competent bodies for the effective addressing of relevant infringements-offences in the context of exchange of information and data, as well as with EU institutions and international organisations.

3.5.20. Availability of reliable identification infrastructure

Assessment rating: Medium (0.5)

Greek citizens over the age of 12 are obligated to have an Identity Card issued by the Hellenic Police²⁰⁸, bear it at all times and produce it upon request by the Police Authorities. Greek Passports are considered equivalent to police-issued identity cards as identification documents.

As Greece is a member state of the Schengen Agreement, identity cards constitute valid documents for travel between the countries of the Agreements.

The Hellenic Police²⁰⁹ is responsible for issuing the main documents certifying identity and, as such, issues police-issued identity cards and passports for Greek citizens.

Police-issued identity cards and other identification documents do not meet current security specifications, while passports, new driving licences²¹⁰ and Hellenic Police personnel identity cards meet strict security requirements.

Greece is an entry point for a large number of migrants and refugees from third countries due to adverse social and political conditions in their countries. Most refugees and migrants enter the country without identification documents.

Applicants for international protection are obligated to deliver their travel documents and any other document in their possession concerning the examination of the application and information certifying their identity and that of their family members, the country and place of origin, as well as marital status. The recognition of the capacity of applicants for international protection does not necessarily require the submission of evidence²¹¹.

²⁰⁶The SEPE was founded by virtue of Law 2639/1998, Gov. Gazette, Series I, 205 'Regulation of labour relations, establishment of a Labour Inspectorate and other provisions', reformed by virtue of Law 3996/2011, Gov. Gazette, Series I, 170 'Reforming the Labour Inspectorate, social security arrangements and other provisions' and Presidential Decree 113/2014, Gov. Gazette, Series I, 180 'Organisation of the Ministry of Labour, Social Security and Welfare', and reports directly to the Minister of Labour, Social Security and Social Solidarity. The Labour Inspectorate is headed by a non-permanent Special Secretary (Article 53 of Presidential Decree 63/2005, Gov. Gazette, Series I, 98), whose post was established by virtue of Article 1 of Law 3996/2011.

²⁰⁷ Article 67A of Law 4387/2016 – Established at the Ministry of Labour, Social Security and Social Solidarity – Unified Social Security Fund (EFKA). By special order of the Governor of EFKA: a. Auditors from any PEKA may carry out audits anywhere within the territory of Greece; b. Joint operations with the participation of more than one PEKA are organised. PEKA operate 24 hours a day, 7 days a week, with proper changeover of personnel, who are obligated to carry out ordinary and overtime work, as well as work on holidays and during night hours, depending on needs.

²⁰⁸ See the website: http://www.hellenicpolice.gr/index.php?option=ozo_content&perform=view&id=139&Itemid=132&lang

²⁰⁹See Joint Ministerial Decision 3021/19/53 dated 14/10/2005 'Type, supporting documents, competent services and procedure for the issuance of identity cards of Greek citizens'.

²¹⁰Issued by the Ministry of Infrastructure, Transport and Networks.

²¹¹ Article 9(1)(b) of Presidential Decree 114/2010, as in force,

For foreign nationals who cannot produce a valid passport, invoking specifically reasoned particular circumstances or conditions in their country of citizenship (objective inability to produce a valid passport), numerous administrative documents²¹² that do not satisfy high security criteria are issued to certify their identity on a case-by-case basis. There is also no single database for the above documents that would allow access to the bodies involved in the context of their competencies.

It is noted that under Law 3907/2011 ‘On the establishment of an Asylum Service and a First Reception Service, adaptation of Greek legislation to the provisions of Directive 2008/115/EC “on common standards and procedures in Member States for returning illegally staying third-country nationals” and other provisions’ all third-country nationals arrested while entering the country without complying with legal formalities are subjected to first reception procedures²¹³.

Additionally, the obligated parties under Law 3691/2008 must apply, as due diligence measures, certification and verification of the identity of customers on the basis of documents, data or information from reliable and independent sources²¹⁴

3.5.21. Availability of independent information sources

Assessment rating: Medium High (0.6)

The standard due diligence measures (Article 13 of Law 3691/2008) applied by the obligated parties with respect to customers include certification and verification of the identity of customers on the basis of documents, data or information from reliable and independent sources²¹⁵.

Of the above independent sources of information, the following are available free of subscription charges and directly accessible through their websites:

- Bar Associations, Courts and the Hellenic Parliament, providing information on the national legislative framework and the case-law of the national courts.
- the Government Gazette (GG/FEK), providing information on all items published by the National Printing Office.
- the General Commercial Registry (GCR/GEMI),²¹⁶ providing information on the incorporation, any amendments, dissolution, liquidation or bankruptcy of legal persons.
- the Independent Authority for Public Revenue (IAPR), providing information on tax and financial data.

The others are independent subscription-based sources and access thereto depends on the needs and the context of the competencies of the obligated parties.

²¹² See Annex ‘Types of Documents’

²¹³First reception procedures for third-country nationals include: a. ascertainment of their identity and nationality; b. registration; c. medical check-up and provision of any care and psychosocial support required; d. provision of information concerning their rights and obligations, particularly the requirements under which they can enjoy international protection status; and e. care for those belonging to vulnerable groups, so that they may be subjected to the applicable procedure. 2. Following a decision by the competent police authorities, third-country nationals who are arrested while illegally residing in the country and who cannot prove their nationality and identity via document issued by a public authority may also be subjected to first reception procedures.

²¹⁴ Article 13 of Law 3691/2008.

²¹⁵‘Tiresias’ S.A. Bank Information Systems, ‘Nomos’ legal database, ‘Nomotelia’ legal database, Hellenic Union of Jurists (eThemis), Nomiki Bibliothiki, LawNet (Legal Search Engines), LawSpot, ‘ISOKRATIS’ (Legal Database of the Athens Bar Association), websites of Bar Associations, Courts and the Hellenic Parliament, the Government Gazette (FEK), the General Commercial Registry (GEMI), the Internet application of the Independent Authority for Public Revenue (IAPR), ICAP, Amadeus and World-Check Risk Intelligence Data.

²¹⁶As of 04/04/2011, it has been operating at the General Commercial Registry Service of the Athens Chamber of Commerce and Industry (ACCI)

By way of indication, in the financial sector obligated parties, in the context of applying customer due diligence (CDD) measures, collect information from independent and reliable sources of information, such as 'Tiresias' S.A. Bank Information Systems, the Government Gazette (GGFEK), the General Commercial Registry (GCR/GEMI) and ICAP, in order to assess their customer's ML/TF risk.

Furthermore, the IAPR uses the 'Amadeus' global subscription-based database, which provides information and financial analysis on the current and past accounting periods of companies, placing emphasis on the profit margin of intra-group transactions.

The Authority uses the 'World Check Risk Intelligence Data' database, a subscription-based platform collecting information at the international level on any natural or legal person.

3.5.22. Availability and access to beneficial ownership information

Assessment rating: Medium Low (0.4)

The standard due diligence measures applied by the obligated parties with respect to customers include the verification of the identity of the beneficial owner(s) of the customer-company, the continuous updating of data and the taking of reasonable measures, depending on the degree of risk, for the validation of their identity data, in order to ensure that the obligated party is aware of the beneficial owner(s).

Article 30 of Directive (EU) 2015/849, which is expected to be directly transposed into national law, provides for the creation of a 'registry' of beneficial owners.

Due to their professional activities, attorneys, accountants - tax consultants and certified public accountants enjoy access to information helping identify beneficial owners in relation to the other obligated parties of the non-financial sector, where the identification of the beneficial owner is particularly hard, particularly in cases of legal persons with a complex or non-transparent structure.

In the gaming sector, there is no legislation providing for the participation of legal persons, trusts or similar structures, except solely the participation of natural persons acting on their account. As such, the beneficial owner and the player are considered to be one and the same.

In the financial sector, a robust regulatory framework²¹⁷ has been enacted, setting out detailed due diligence measures for the identification of beneficial owners and their equivalent treatment as customers.

More specifically, there is provision for the submission of a declaration by legal representatives for the beneficial owner of the legal entity they represent and for whom they are entering into transactions, accompanied by the identification documents of the beneficial owner.

²¹⁷ Decision No 281/2009 of the Banking and Credit Committee of the Bank of Greece and Decision No 1/506/ 2009 of the Board of Directors of the Hellenic Capital Market Commission.

4. BANKING SECTOR

4.1. Summary

The Banking Sector is significant for the Greek economy, as the total assets (before accounting provisions) held by the 39 Credit Institutions (CIs) amounted to 360,1bn euros in 2016, around two times the country's GDP of 176 bn euros. Four (4) significant CIs concentrate the large majority of the Banking Sector's activity (93,5% of total Assets).

The overall ML Risk in the Banking Sector is Medium High, assessed as a combination of the ML Threat and the ML Vulnerability of the sector. The Banking Sector faces a High level of ML Threat, being traditionally a target of criminals in their effort to launder the proceeds of crime due to its significant size and the large volume of transactions. The Overall ML Vulnerability of the Banking Sector is assessed as Medium, based on the quality of the General AML Controls in place and the Inherent Vulnerability of eleven banking products, analyzed according to the methodology of the World Bank.

There are some contextual factors affecting both the Threat and the Vulnerability of the Banking Sector that should be placed on top of the detailed assessment of the General AML Controls and Products' Vulnerabilities. In particular, the imposition of capital controls in July 2015, has, notwithstanding its adverse economic impact, a mitigating effect on the ML risk (especially that arising from tax evasion) and favors card usage and electronic transactions. Furthermore, the development and use of powerful tools from the tax authorities, aiming to tackle tax evasion (such as electronic reporting of an extensive range of CIs customers' transactions and direct access to the registry for bank accounts) further reduce the attractiveness of the Banking Sector to money launderers.

The first component of the assessment of Overall ML Vulnerability of the Banking Sector refers to General AML Controls, which are assessed as Medium High, taking into consideration the following:

- The Banking Sector has been subject to a robust legal and regulatory AML/CFT framework, which has introduced on top of CDD measures applicable in other EU countries, additional provisions aiming to detect customers vulnerable to tax evasion and report their suspicious transactions to the Hellenic Financial Intelligence Unit (FIU). The Executive Director of IMF Mrs Christine Lagarde referred to the positive results of these provisions in a speech addressed to FATF's Plenary in June 2016²¹⁸. Nevertheless, the regulatory framework needs to be further strengthened and oriented towards a more effective application of the risk-based approach in line with the new AML Law transposing Directive (EU) 2015/849, as soon as the latter is enacted.
- AML/CFT supervision benefits from the synergies and the solid requirements of prudential supervision's framework outlined in the Banking Law 4261/5.5.2014 which transposed Directive 2013/36/EU (Capital Requirements Directive IV) and a broad set of European Banking Authority's guidelines endorsed. Although the conduct of AML/CFT supervision remains a national competence, the conduct of prudential supervision in close collaboration with the Single Supervisory Mechanism since November 2014, on the basis of strict pan European standards and methodologies, has proven to be a strong additional component of an effective identification, understanding and assessment of ML, compliance and reputational risk.
- AML/CFT supervision of the Bank of Greece is risk-based, conducted through a Risk-Based Off-site Analytical Tool (RBOAT), developed under the technical assistance of IMF in 2013. The number of on-site

²¹⁸<http://www.fatf-gafi.org/publications/fatfgeneral/documents/speech-imf-md-22june2017.html>

inspections in the last 5 years are deemed adequate, considering the current landscape of the banking sector and the concentration of 93,5% of bank assets to the four (4) significant CIs. Although the AML Section's personnel consists of qualified experienced examiners, additional staffing would be appropriate, considering the different sectors and the number of supervised entities. In addition the provision of adequate training to AML/CFT examiners should be an on-going priority to foster the effective application of risk-based supervision.

- The type and the amount of administrative sanctions imposed in the past both to CIs and senior management indicate their effective, proportionate and dissuasive nature. The same applies for criminal sanctions, considering specific cases of criminal proceedings against Bank executives and in particular felony charges filed against a prominent former Banker.
- AML Training of CIs' staff should be prioritized, considering the need to apply effectively the risk-based approach. Although Compliance Units usually receive targeted training, front line employees, as well as employees of specific units (large corporates, private banking etc) mostly lack specific AML training focused on the particular characteristics/inherent vulnerabilities of the products/services they provide.
- The Effectiveness of Suspicious Activity Monitoring and Reporting is based on CIs' specific AML IT systems which perform the basic operations of risk profiling, transaction monitoring and sanctions screening, as well as the detection of PEPs. STRs submitted by CIs accounted, on average, for approximately 41% of total STRs of the financial sector in the last five years. Although the quality of STRs has also improved in the last three years, deficiencies in the analysis of cases and supporting documentation still remain. The development of a feedback process from the FIU to the CIs would contribute further to the improvement of the STR quality and their ability to identify suspicious transactions or activities. Feedback could involve reviews of specific cases reported, as well as strategic analysis of overall risk-based conclusions (i.e. trends on suspicious activity typologies or high risk sectors, best practices etc.).
- Availability and access to Beneficial Ownership Information is one of the most important requirements stemming from the 4th AMLD. The draft law provides for a beneficial owners' registry, for storing the beneficial owner information of every legal entity incorporated in Greece. CIs have had for quite some time the obligation to verify the identity of the beneficial owner of the legal entities that hold accounts with them and maintain relevant information in their customer files. Nevertheless the set up and effective operation of the UBO registry should be a top priority which will significantly assist them carry out more effectively their CDD obligations.

In terms of the Inherent Product Vulnerability, the Greek Banking Sector is predominantly made up of commercial CIs, involved in traditional banking services (deposits, loans, payment services), while Investment Banking services are limited. Banking services are largely provided through the extended branch network of the CIs, while alternative services channels (internet or mobile banking), have relatively recently expanded. The analysis of the banking products did not reveal significant ML vulnerabilities, as their assessment ranges from low to medium. In all cases the Inherent ML Risk is considered to be effectively mitigated either through product - specific AML Controls or other factors such as lack of anonymity, lack of agents, very limited omnibus use of deposit accounts, advanced IT monitoring/tracing systems. The two more vulnerable products are, mainly due to their nature: a) Safe Deposit Services, although they are offered to a tiny percentage of natural persons under the condition that they hold a deposit account in the CI, b) Private Banking Services, although they are offered only by the four significant CIs to a relatively small percentage of customers and have been largely limited due to capital control on outgoing cross border credit transfers. From the rest of the products, Deposits,

notwithstanding the decline in terms of outstanding balances and transactions, remain the most significant product offered by CIs, facing ML threats related with several ML typologies, especially in the placement stage. The ML vulnerability of cheques (personal, not bank cheques) mainly derives from their traditional alternative use in Greece as a credit instrument for business to business transactions allowing for anonymous or/and difficult to trace use (e.g. issuing as payable to bearer, post – dating and intermediary endorsements), which makes them vulnerable to fraud or trade-based ML schemes through fictitious invoices. Lending activity has been harshly hit from the economic crisis and the challenges CIs face (more than 44% of credit facilities fall within Non-Performing Exposures), so the risks are reduced and have shifted from new financing to loan restructurings. Correspondent Banking Services are offered on a very limited scale by Greek systemic CIs, mainly to their cross-border subsidiaries, while CIs use Correspondent Services that are largely (90%) offered by major correspondents (belonging to Wolfsburg Group) with tight AML standards.

4.2. Banking sector overview

The Banking Sector is very significant for the Greek economy, as total assets (before accounting provisions) held by Credit Institutions (hereafter CIs) in 2016 amounted to 360,1bn euros, around two times the country’s GDP of 176 bn euros. Moreover, CIs perform the large majority of payments, amounting to 693bn euros for 2016.

As of 31.12.2016, the Banking Sector consisted of 39 CIs. In more detail, four significant CIs concentrate the large majority of the Banking Sector’s activity (93,5% of total Assets), 2 less significant institutions (LSIs) offer a wide range of products, 23 LSIs have limited and specialized activity (e.g. specific lending, investment services) and 9 LSIs are cooperative banks with a limited local spectrum. The banking landscape in Greece is quite different from that prevailing five years ago, as indicated in the following Table (amounts in billion euros)

BANKING SECTOR INFORMATION	2012	2016	Var%
Gross Domestic Product	191 €	176 €	-7,8%
Number of Credit Institutions	52	39	-25,0%
Number of Branches	3.629	2.332	-36,0%
Number of Employees	57.006	42.628	-30,4%
Total Assets	441,4 €	360,1€	-18,41%
Assets Concentration in the four Significant CIs	79,9%	93,5%	+13,6 p.ps
Value of Payment Transactions through CIs	1.078,3 €	692,9 €	-35,7%

Table 31- Statistics on the banking sector for the years 2012-2016

During the first years of the economic crisis, Greek CIs were cut - off from international markets and, until June 2012, experienced an unprecedented outflow of deposits, equivalent to one third of their deposit base. In response, they resorted increasingly to short-term financing from the Euro-System (close to €140

billion in June 2012). In addition, the heavy losses they suffered from 2010 onwards and especially the impact of Private Sector Involvement (PSI) resulted in a capital shortage for nearly all CIs at the end of 2011. Their recapitalization became imperative in order to fully protect depositors. Under these adverse circumstances, the government and the Bank of Greece took a number of actions safeguarding financial stability. The most important involved the resolution of weak CIs under a new legal framework and the recapitalization of core CIs. By the end of 2013, twelve CIs as well as the Cypriot CI's branches had been resolved / transferred (healthy assets) to the significant CIs. The restoration of significant CIs' capital adequacy ratios has required three recapitalization processes since then, that took place in 2013, 2014 and 2015 respectively. In the meanwhile, excess employees and branch capacity have largely been eliminated and fewer but stronger CIs are in operation (in particular four significant CIs), benefitting from synergies and economies of scale, including in terms of AML/CFT systems and controls.

4.3. Specific characteristics of the greek banking sector

4.3.1. Capital controls

During the second quarter of 2015, Greece found itself at the end of the established bailout period without having reached an agreement with its creditors on further expansion of the program. This fact increased the political uncertainty of the country, which had already caused a significant outflow of deposits from the Greek banking system during the first semester of 2015. Therefore, the European Central Bank decided not to proceed with a further increase of the level of Emergency Liquidity Assistance (ELA) provided for Greek CIs. As a result, the Greek government had to introduce a bank holiday period for almost 20 days (from 28/6 to 20/7/2015) and to impose capital controls, which included inter alia, the following provisions: a) credit transfers abroad permitted up to a monthly threshold of €1.000 per person per CI, b) cash withdrawals permitted up to a daily threshold of €60 per person per bank (monthly threshold of €2.300 since 1/3/2018), c) particular due diligence required for the execution of large commercial credit transfers abroad (detailed documentation and justification).

Businesses and consumers have adapted to a great extent to the conduct of payments without the use of cash, since the implementation of capital control measures, as evidenced by the following data (as of end of 2017):

- Numbers of point-of-sale (POS) terminals have increased considerably by 312.459 (+87%).
- Paymentcard transactions increased by 245,2 million (+79%) and electronic credit transfers by 24%.
- The value of payment card transactions has increased by €7,1 billion (+45%).
- The value of Internet and mobile banking transactions has increased by 29% (+€11,2 billion) and 82% (+€359 million) respectively.

Based on the above, capital controls, apart from their adverse economic impact, have a mitigating effect in terms of the ML risk (especially that arising from tax evasion risk), as they favor card usage and electronic transactions.

4.3.2. Tax evasion

The fight against tax evasion was set up as a national top priority during the crisis and many tools have been provided to the tax authorities for this purpose. In particular:

- Credit institutions report annually an extensive range of their customers' transactions (credits or debits exceeding 100.000 per year, cross border credit transfers etc) directly to the tax authorities through secure electronic means (Ministry of Finance Decision POL 1033/2014).
- Tax authorities (as well as judicial authorities and the FIU) have access to the accounts and transactions of Cls' customers subject to tax audit, through the registry for bank and payment accounts introduced by Law 4170/2013. The same infrastructure has also been used for cumulative inquiries on large numbers of bank customers subject to tax audits.
- Tax authorities made 4.930 reports to the FIU for tax crimes in 2015 and 2016, and the latter proceeded to the freezing of tax evaders' bank accounts/property on a materiality basis.
- Electronic seizures orders of bank accounts' balances have been widely used by tax and social security authorities to collect tax/social security debts.
- Greece belongs in the pool of 49 jurisdictions undertaking first Automatic Exchange of Financial Accounts Information in 2017 under the Common Reporting Standard (CRS) of OECD. In this respect, information regarding assets held by foreign tax residents in Greek Cls will be provided to foreign tax authorities which will mutually inform Greek tax authorities about assets held by Greek tax residents in their jurisdictions.

The above strict tax controls reduce the attractiveness of the banking sector for ML purposes.

4.3.3. Cash activity

Cash in circulation (banknotes and coins) in Greece has increased steadily since 2012, to the amount of 30.728 million in December 2016 (Dec. 2015: 29.571, June 2015: 28.450, Dec. 2014: 27.928, Dec. 2013: 25.391). At the same time, the cash transactions (deposits, withdrawals) performed through the Banking Sector have significantly decreased (-80% since 2012, -50% since 2014). The above facts indicate the existence of a growing cash-based economy and are an additional indication of the reduced attractiveness of the banking sector for ML purposes.

Furthermore, a number of legislative measures have been taken to reduce the use of cash and tackle tax evasion. In particular, based on Law 4446/2016, all transactions between private individuals and businesses (for the sale of goods or the provision of services) exceeding €500 (the previous threshold was €1.500) have to be conducted exclusively by payment cards (debit, credit, prepaid) or other electronic means of payment (e.g. credit transfers, direct debits). The above threshold is the lowest in the European Union, according to the Supranational ML/TF Risk Assessment Report (SNRA) of the European Commission published on 26.6.2017. Law 4446/2016 includes additional provisions for promoting electronic payments.

4.4. Banking sector vulnerability

The Overall ML Vulnerability of the Banking Sector is assessed as Medium, based on the quality of the General AML Controls in place and the inherent vulnerability of eleven banking products, analyzed according to the methodology of the World Bank. In particular, the overall vulnerability rating derives from the assessment of General AML Controls (Medium High) and from the Product/Service Vulnerability which changed from Low to Medium.

4.4.1. General AML controls

Assessment rating: Medium High

The assessment is based on a synthetic analysis of 13 input variables, which are presented in the following sections. The goal of the analysis was to assess whether the Credit Institutions are sufficiently willing, informed, able and effective in their efforts of managing ML/FT risk.

GENERAL INPUT VARIABLES		ASSESSMENT RATING
1	Comprehensiveness of AML Legal Framework	High
2	Effectiveness of Supervision Procedures and Practices	High
3	Availability and Enforcement of Administrative Sanctions	High
4	Availability and Effectiveness of Entry Controls	Close to Excellent
5	Integrity of Leadership and Banks' Staff	High
6	Availability and Enforcement of Criminal Sanctions	High
7	Level of Market Pressure to Meet AML Standards	High
8	Effectiveness of Compliance Function	High
9	AML Knowledge of Banks' Staff	Medium High
10	Effectiveness of Suspicious Activity Monitoring and Reporting	Medium High
11	Availability and Access to Beneficial Ownership Information	Medium
12	Availability of Reliable Identification Infrastructure	Medium
13	Availability of Independent Information Sources	Medium High
GENERAL AML CONTROLS		Medium High

Table 32- Banking Sector: Assessment of general AML/CFT controls

* The variables 11-13 are assessed as variables 1.3.20-.1.3.22 in the chapter of National Vulnerability

4.4.1.1. Comprehensiveness of AML legal framework

Assessment rating: Medium High

Greece has a robust legal and regulatory framework which follows FATF and EU developments. In particular, the AML/CFT legal framework is based on Law 3691/5.8.2008 (AML Law), which transposed the provisions of Directive 2005/60/EC (3rd EU AML Directive) and has significantly strengthened ever since, through several amendments. The most important of these amendments took place under the on-going monitoring of FATF which terminated the follow-up process of Greece in October 2011, as it concluded that the country had implemented all core and key Recommendations at a level essentially equivalent to C (Compliant) or LC (Largely Compliant).

The Bank of Greece is the competent authority for CIs and is given by virtue of para. 2 and 3 of article 6 of the AML Law the appropriate regulatory and supervisory tasks and powers. The Bank of Greece has specified AML/CFT requirements for credit institutions by issuing Decision 281/5/17.3.2009 of the Banking and Credit Committee (hereafter Decision 281/2009), which sets out requirements with regard to customer and UBO identification and verification, record keeping, on-going monitoring and suspicious transactions reporting, tipping off and confidentiality, internal controls, foreign branches and subsidiaries, third parties reliance etc. The Bank of Greece has also issued Decision 285/6/9.7.2009 of the Banking and Credit Committee, which is an indicative typology intended to provide guidance to credit institutions for the detection of suspicious or unusual transactions, including a specific category for transactions possibly related to tax evasion.

The above two Decisions have been supplemented by Bank of Greece's Governor's Act 2652 issued on 29.2.2012 Governor's Act 2652, which were drafted with the IMF under the technical assistance of IMF

and were included as Prior Actions in the MoU between Greece and the Institutions (EC, ECB and IMF) with the aim to detect customers vulnerable to tax evasion and report their unusual transactions to the FIU. It is worth noting that on top of the CDD requirements imposed in other EU/FATF countries, credit institutions are obliged, based on the above Act, to verify their customers' income through their latest tax clearance or tax declaration form, as part of their economic/transacting profile.

It should also be highlighted that Decision 281/2009 puts great emphasis on the proper identification and management of ML/TF risk, setting strict requirements to the CIs. CIs, in the context of an effective risk management strategy, have to adopt an AML/CFT policy, which has to be recorded, documented and approved by the Board of Directors. As part of this policy, CIs are obliged to adopt policies and procedures for the timely and proper identification and assessment of ML/TF risk (chapter 4 of Decision 281/2009).

CIs conduct the appropriate customer due diligence (CDD) measures and they have to justify to the Bank of Greece that the scope of the relevant measures is proportionate to the ML/FT risk, as well as that they apply these measures consistently and effectively. The appropriate procedures and measures applied for managing ML/FT risk have to be determined on the basis of the size, structure and complexity of each CI's operations. Clients are classified in three risk categories: low, medium and high risk, associated with appropriate CDD, periodic monitoring and control measures. Risk assessment should include at least the following parameters: professional/business activity, customer's economic/ transacting profile, customer's home country or country of business, legal status and country of incorporation of a legal person, complexity of corporate structure, countries of origin and destination of funds, complexity of transactions, volume, size and kind of business transactions, transactions with the use of new technologies. On top of their risk assessment, CIs are required to apply enhanced CDD measures for the following 11 high-risk customers' categories: non-residents, political exposed persons (including domestic ones), companies with bearer shares, offshore companies/special purpose vehicles, trusts, non-profit organizations, private banking, non-face-to-face transactions, cross-border correspondent banking relationships, high-risk countries, business relationships and transactions that entail high risk of tax evasion (self-employed with total primary credits exceeding €200.000 and legal persons whose cash deposits or cash withdrawals exceed €300.000 per year).

It should be noted that a Law Making Committee has finalized the draft law that transposes the provisions of Directive (EU) 2015/849 and further improves the existing framework fully aligning it with the revised FATF Recs of 2012 and the EU strict new provisions (which go further from FATF Recs in some areas). The draft law introduces the following main developments:

- Enforces further development of the risk-based approach towards AML/CFT, as a more effective way of identifying and mitigating ML/FT risks.
- Requires the development of a beneficial owner registry for any type of legal entity established in Greece. Legal entities based in Greece are required to keep adequate, accurate and updated information on their beneficial owners.
- Imposes stronger checks on risky third countries by the development of a "blacklist" of third countries posing a risk to the EU financial system.
- Imposes stricter penalties on the obliged persons related to the financial sector, distinguishing them from the rest.

The above is supplemented by Regulation (EU) 2015/847 on information accompanying transfers of funds which has been applied since the 26th of June 2017, and further strengthens the payments' framework as:

a) transfers of funds shall be accompanied by information on the payee, not only the payer and b) the

payment service provider of the payee and the intermediary shall establish effective risk-based procedures for determining whether to execute, reject or suspend a transaction lacking the required information. Moreover, the regulatory framework is supplemented by the Regulatory Technical Standards (directly applicable in all EEA countries).

The Bank of Greece has planned the necessary amendments of the regulatory framework to fully align it with the new AML Law. The amendments will set the ground for a more effective application of the risk-based approach, taking the Risk Factors Guidelines issued by the European Supervisory Authorities.

4.4.1.2. Effectiveness of supervision procedures and practices

Assessment rating: Medium High

AML/CFT supervision framework

AML/CFT supervision of credit institutions has been assigned to the Bank of Greece by virtue of par. 2 of article 6 of Law 3691/2008 (AML Law). It forms an integral but distinct part of prudential supervision which, according to the Bank's Statute and the Banking Law 4261/2014 is one of the main tasks of the Bank of Greece. The later has full administrative, operational and financial independence which ensures its capability to fund and exercise adequately all the tasks that are defined by its Statute and the Greek legal framework.

Based on the 10th follow-up report of FATF for Greece, on the basis of which Greece has been removed from the follow-up process, the country has undertaken sufficient action to address the shortcomings related to R23 (supervision) and reached a satisfactory level of compliance.

In April 2014, AML/CFT supervision has been moved to the AML Section of the newly established Supervised Institutions Inspection Department, which was set up in order to respond to the Single Supervisory Mechanism structure and the need to focus on on-site inspections. The AML Section: a) follows European and international developments and institutional issues and elaborates AML/CFT guidelines addressed to the supervised institutions, b) develops audit tools and assesses the adequacy of the procedures of the supervised institutions on an off-site basis, c) carries out on-site inspections based on its risk-based supervisory program presented below. The AML Section works in close co-operation with the IT Auditing Section that examines the AML/CFT IT systems infrastructure of each CI as part of its duties.

The AML Section counts 9 qualified examiners, with an auditing experience of 10 years on an average, with economics/finance university postgraduate degree, computer skills and an excellent command of English. Qualified examiners from the On-site Inspections Section and the IT Auditing Section take part several times in the AML/CFT on-site inspections in order to strengthen the supervisory teams with complementary expertise. The Bank of Greece's examiners are required to maintain high professional standards, as, according to Article 55C of the BOG Statute, forbidden to disclose to any natural person or legal entity and to any public authority the information or data reported. The AML/CFT training of the staff is set out as a high priority. The AML Section's examiners regularly attend specialized seminars. In addition, significant expertise and knowledge is acquired through the participation of the Section in FATF, AML Committee of the European Supervisory Authorities and the EU Expert Group on ML/TF. The developments and the technical papers shared within these fora are communicated to AML Section's examiners and contribute to the on-going strengthening of their expertise.

Nevertheless, in the Supranational ML/TF Risk Assessment Report (SNRA) of the European Commission published on 26.6.2017, emphasis was placed upon the need to further build supervisory capacity. The above

suggestion applies for the Bank of Greece, considering the different sectors and the number of entities supervised, as well as the range of its tasks.

Off-site Supervisory process

AML/CFT supervision is risk-based and has been designed according to FATF's Risk-Based Approach for the Banking Sector issued in October 2014. The Bank of Greece has notified the European Banking Authority that it considers it complies with the Risk-Based Supervision Guidelines issued by the European Supervisory Authorities in November 2016.

The basic tool of AML/CFT supervision is the Risk-Based Off-site Analytical Tool (RBOAT) developed in 2013 with the IMF under a Technical Assistance Program. RBOAT is a sophisticated risk matrix that aims to identify and assess ML/TF risks of each credit institution and formulate its institutional risk profile. There is a detailed manual regarding the operation of the RBOAT, but in a nutshell, the RBOAT includes the following components: a) assessment of structural risk factors, b) identification of significant business activities, c) assessment of the inherent ML/TF risk of these activities and d) evaluation of ML/TF risk mitigation controls. In order to assess the structural risk factors the AML Section receives relevant information from the Banking Supervision Department which shares its assessment on structural elements/ changes from the previous year. CIs submit twice a year, electronically, a standardized data gathering form, with the required data for the assessment of their inherent risk, and an Annual Report of the AML Officer for the assessment of their ML/TF risk mitigating controls. Additional reports regarding compliance and internal control systems prepared internally, as well as by external auditors, are also analyzed in the context of on-going AML/CFT supervision. The results of the off-site risk assessment are used to properly decide on the supervisory actions and the allocation of AML/CFT supervisory resources, including decisions about the focus, depth, duration and frequency of on-site and off-site activities.

On-site inspections

The program of on-site inspections is based upon the off-site rating described above and additional supervisory information (e.g. from annual AML/CFT reports, previous on-site reports, special incidents, information from Banking Supervision Department, feedback from FIU). The duration of the inspection ranges from two to eight weeks, according to the size, complexity of operations, scope of the inspection and AML/CFT risk of the CIs. On-site inspections are conducted according to the inspection-manual of the AML Section, which specifies, in an analytical manner, the procedures for the various areas of inspection.

44 on-site inspections have been conducted from 2012-mid 2017, according to the on-site risk-based examination procedures which are scheduled to allow the examiners to validate the results of the RBOAT and the institutional risk profile assigned. This number should be read in conjunction with the significant consolidation arisen in Greece during the crisis (four significant banks represent 93,5% of the banking sector in terms of assets). It is worth mentioning that 9 of these on-site inspections were carried out in the largest banks as part of a prior action included in the MoU between Greece and the Institutions, which required the assessment of compliance with the provisions introduced by Bank of Greece Executive Committee Act 2652/2012 aimed to detect customers vulnerable to tax evasion and report their unusual transactions to the FIU. In these on-site inspections the supervisory teams reviewed a targeted sample of 300 customers per bank (2700 in total) under the close monitoring of IMF which assessed the whole thematic project as a very successful one.

Offsite supervision and onsite inspections indicate an adequate level of awareness, identification and management of ML/TF risks by CIs. In addition the large concentration of the Banking Sector in the 4 significant

CIs, creates economies of scale in AML/CFT operations and controls, while their direct supervision by the SSM has strengthened their corporate governance and internal control systems.

4.4.1.3. Availability and enforcement of administrative sanctions

Assessment rating: High

The AML legal and regulative framework provide for the imposition of severe administrative sanctions in cases of non-compliance with AML obligations. The range of sanctions is sufficiently broad to achieve the right balance between effectiveness, dissuasiveness and proportionality, as it includes corrective measures, fines, removal of staff or suspension of certain activities. In particular, the administrative sanctions as set out in art. 52 of the AML Law include:

- a fine on the legal person of €10.000 to €1.000.000 and, in case of recidivism, of €50.000 to €2.000.000;
- a fine of €5.000 to €50.000 on the managing director, the members of the board of directors, management officers or other employees of the legal person who are responsible for the violations or exercise of insufficient control and supervision of the services, the employees and activities of the legal person; in case of recidivism, a fine of €10.000 to €100.000 shall be imposed;
- removal of the directors, the managing director, management officers or other employees for a specific time period and prohibition of assuming other important duties;
- prohibition of the legal person from carrying out certain activities, establishing new branches in Greece or abroad or increasing its share capital;
- In case of serious and/or repeated violations, final or provisional withdrawal or suspension of authorization of the corporation for a specific time period or prohibition to carry out its business.

The administrative sanctions are justified and publicized provided that their publication is unlikely to cause disproportionate damage to the legal person on which the sanction is imposed. The administrative sanctions of art. 52 are independent from the much harsher sanctions listed in Article 51 which refer to the liability of legal persons, where any of the money laundering offences is committed for the benefit of the obliged legal person by a physical person acting either individually or as part of an organ of the legal person (including fines from €50.000 to €5.000.000 euros).

The Bank of Greece has also issued, in accordance with par. 3 of article 52 of the AML Law, Decision 290/12/11.11.2009 of the Banking and Credit Committee governing the imposition of administrative sanctions on institutions supervised by the Bank of Greece, which specifies: i) the degree of importance of the individual obligations of SIs, their managers and staff, by type of obligation and ii) the criteria for specifying the administrative sanctions to be imposed on the above persons, in cases of non-compliance with their obligations arising from the legislation in force. This Decision constitutes, in addition to Decision 281/2009, an important tool in the BOG's AML/CFT supervisory powers, because it specifies in an exhaustive way and classifies by order of importance all individual AML/CFT requirements whether applicable to the legal person concerned or its employees.

It should be noted that the Bank of Greece has also issued Decision 300/30/28.7.2010 which introduces sanctions for credit and financial institutions for failure to promptly apply freezing requests or respond without delay to orders to seek and identify suspected terrorist assets.

The administrative sanctions of article 52 have been imposed in a number of cases, taking into account the criteria of Decision 290/12/11.11.2009, on credit institutions or on their staff. In particular, during the last 5 years the following sanctions have been imposed through Decisions of the Banking and Insurance Committee: a) 34 corrective measures in 9 credit institutions, b) total fines of €2.909.000 on 17 credit institutions, c) total fines of and €1.195.000 on 9 senior management employees, d) two removals of senior management employees. Follow up inspections and other supervisory audit procedures allow for the monitoring of the proper and timely implementation of corrective measures. The type and the amount of administrative sanctions imposed both to CIs and senior management indicate their effective, proportionate and dissuasive character.

4.4.1.4. Availability and effectiveness of entry controls

Assessment rating: Close to Excellent

Entry controls in the Banking Sector are ensured by the robust EU framework which has been significantly strengthened since June 2013 through the issuance of Directive 2013/36/EU (Capital Requirements Directive IV) and Regulation (EU) 575/2013 (Capital Requirements Regulation). The relevant transposition Law 4261/2014 includes, inter alia, provisions on: establishment and operation of credit institutions, freedom of establishment and provision of services by credit institutions, prudential supervision rules, powers of supervisory authorities and administrative penalties they may impose on credit institutions, corporate governance of credit institutions, remuneration policy implemented by credit institutions, introduction of capital buffers to be maintained by credit institutions.

To achieve its supervisory objectives, the Bank of Greece has issued the Executive Committee Act 22/12.7.2013, setting the procedures for the authorization of credit institutions in Greece and for the acquisition of a holding in an existing credit institution, including the prudential assessment of the liable persons. This Act takes into account, inter alia: a) Bank of Greece Governor's Act 2577/9.3.2006 on the framework of operational principles and criteria for the evaluation of the organization of Internal Control Systems of credit and financial institutions and relevant powers of their management bodies, b) the European Banking Authority (EBA) Guidelines on the assessment of the suitability of members of the management body and key function holders (EBA/GL/2012/06) and the relevant guidelines for the prudential assessment of acquisitions and increases in holdings in the financial sector.

The Banking Supervision Department has the necessary resources to perform its duties effectively regarding the authorization and supervision of CIs in close collaboration with the ECB acting within the context of the Single Supervisory Mechanism, which, since its launch in November 2014, has significantly strengthened prudential supervision.

In the last 5 years only 5 requests for the establishment of foreign CIs have been made, due to the fiscal crisis and the difficulties faced by the Greek economy and the banking sector. Four regarded the establishment of EU CIs' branches (mainly their conversion from representative offices to branches) and one regarded the request to establish a new CI in Greece (rejected due to insufficient documentation).

In Greece, the Hellenic Financial Stability Fund (HFSF), operating in line with "HFSF Law" 3864/2010, is an additional controlling factor for the quality of the corporate governance of the four significant CIs that

have received capital support in the past from the state. The signed bilateral Relationship Framework Agreements provide, among others, significant controlling powers to HFSF in terms of corporate governance (iecomposition of the Executive Committee, quality of key function holders, and other material organizational transformations, mergers, restructurings, capital changes etc.)

4.4.1.5. Integrity of leadership and staff

Assessment rating: High

As mentioned above in the Entry Controls Section, the Greek Banking Law (4261/2014), the relevant Decisions of the Bank of Greece and the European Banking Authority's Guidelines provide for strict fit and proper criteria for the shareholders (including the beneficial owner), members of the management body and key function managers. The Bank of Greece jointly with the SSM, contributed significantly, in the past years, in strengthening the governance of both significant and less significant CIs, in the context of required skills and competence for facing the adverse economic environment, as well as the efficiency of their organizational structure.

There are several controls or practices in the Banking Sector that promote Staff Integrity, such as hiring practices that involve mandatory fitness and propriety checks (penal record at a minimum), contract termination terms related to the adherence of ethical principles (policies against conflict, code of conduct, AML etc), ongoing vetting programs that focus both on theoretical and real corruption incidents and secure processes for anonymized reports regarding suspicious, unethical or illegal behavior, directed either to the Internal Audit or the Compliance Function.

In the 5-year period 2012-2016, the CIs identified approximately 600 operational risk incidents that resulted in disciplinary action ranging from a simple reprimand to dismissal. In 192 cases they terminated the working relationship with the employee, out of which, in 43 cases they also initiated legal actions against them. Based on analytical regulatory reports for the aforementioned period, the above incidents were identified mainly in CIs' branches. Taking into consideration the overall number of employees in the Banking Sector (more than 48 thousand on average between 2012-2016), as well as the downward trend of the incidents in 2016 (-54% compared to 2012 and -21% compared to 2015) the above numbers are indicative of a strengthened control environment against fraud.

4.4.1.6. Availability and enforcement of criminal sanctions

Assessment rating: High

The legal framework of criminal sanctions against employees or executives of CIs that are involved in ML/FT offenses is specified in article 45 of the AML Law 3691/2008, while criminal sanctions are also applicable for appropriate ancillary offenses to ML. The above legal framework stipulates punishment of deprivation of liberty up to 20 years and fines from 20.000 to 1.500.000 euros for persons who have committed money laundering, as well as increased sanctions in cases of recidivism.

AML Policies of the Banking Sector generally describe the legal ramifications for the employees or executives, in case they are involved in ML /FT related offenses.

The recent history of legal actions against Bank executives in combination with several special investigations performed by the Bank of Greece are considered to be adequately dissuasive factors that have increased the overall awareness of the Banking Sector regarding the importance of the AML Law. In particular:

- a) There have been several criminal proceedings against Bank executives or employees related to offenses stated in Article 3 of the AML Law since 2010, such as:
 - The most prominent case refers to criminal charges against a former banker and CEO, as well as eight executives of one CI for fraud, embezzlement, criminal misconduct related to corporate loans and ML. Although the case has not been brought to court, the former banker has been imprisoned.
 - Criminal charges against the former CEO and several Bank executives of one CI for fraud, criminal misconduct related to corporate loans and ML. The case is pending.
 - Criminal charges against the previous owner of a CI for fraud, criminal misconduct regarding loans to shipping companies and ML. He was acquitted.
- b) The judicial authorities have also taken measures (approximately 40 cases of account freezing or requesting a lift of banking secrecy), in the context of their investigations.
- c) Several special investigations regarding corporate loans have been performed by the Bank of Greece in the previous years based on requests from judicial authorities. In one case, criminal charges were filed against executives of a CI for criminal misconduct regarding corporate loans. The case is pending.

Finally, during the last 5 years, in 43 cases criminal proceedings were initiated against employees mainly for embezzlement. In some of these cases, identified through queries in legal databases, the criminal charges regarding the ancillary offenses were accompanied with charges for ML.

4.4.1.7. Level of market pressure to meet AML standards

Assessment rating: High

AML/CFT standards produced at international level by the Financial Action Task Force (hereinafter 'FATF') constitute, by common accord, international "soft" law of particular importance, given that they constitute a "regulatory benchmark" to which all countries tend to comply through proactive adaptation, periodical FATF assessments, IMF Financial Sector Assessment Programs and market pressure from cross-border business relations of CIs. At a country level, the unsuccessful adoption and implementation of FATF standards may lead to a high risk classification, with extremely adverse consequences for the domestic banking system.

At a CI level, market pressure for the adoption of FATF AML/CFT standards is mainly applied through "correspondent banking" services, through the introduction of stricter KYC control procedures or mechanisms. CIs operating in Greece maintain relations mainly with large correspondents, members of the Wolfsburg Group (90%), or CIs residing in European Union, USA, Canada and Australia. For the above reason, significant market pressure has been exerted upon them for complying with the stringent international requirements. According to the 10th ECB survey on correspondent banking, published in February 2017, the regulatory requirements related to KYC and AML/CFT has resulted in de-risking strategies from the leading correspondents, who are no longer willing to accept risks that might affect their reputation and profitability. As a result, correspondent activity tends to be concentrated in large correspondents, that:

- a) Require more analytical and regularly updated information in relation to the compliance with international AML/CFT standards. The required information is not limited to the typical Wolfsburg questionnaire, but often includes thematic questionnaires (i.e. regarding International Financial Sanctions) or extended and analytical descriptions of internal AML/CFT processes. Some issues are often clarified through teleconference meetings.

- b) Pose restrictions on the use of correspondent accounts towards specific categories of transactions or customers such as high risk countries, embassies, cryptocurrency, gambling, scholarships, money remitters, travel/ tourism agencies, etc.
- c) Tighten AML/CFT transactional controls. The correspondent reserves the right to deny transactions or delay them upon receiving satisfactory justification (documents, certificates, invoices, contracts etc.)

4.4.1.8. Effectiveness of compliance function

Assessment rating: Medium High

Decision 281/2009 sets out detailed requirements for the AML Officer and the Compliance Function (Special AML/CFT Service), including a detailed reference to their duties and a number of requirements regarding independence, Human/IT resources, AML/CFT policies and controls/audit procedures, reporting etc.). Additionally, CIs are required to have strong and effective corporate governance and Internal Control Systems, based on the CRD IV which has been incorporated into the Greek Banking Law 4261/2014 and the Bank of Greece Governor's Act 2577/9.3.2006 (i.e. segregation of duties, four eyes principle, existence and independence of compliance and internal audit function etc.)

Based on a risk - weighted assessment of nine (9) CIs representing approximately 99% of the Banking sector activity, the Compliance Function is deemed quite effective in terms of its organization and the execution of its duties. In particular:

- a) The AML Officers (and their deputies) have been appointed by the Board of Directors, fulfil the strict fit and proper requirements and they have in general sufficient professional qualifications. They have the necessary independence as well as adequately defined duties according to the regulatory framework.
- b) The average number of personnel working in the AML/CFT Service is deemed sufficient, with a shortage of staff being recorded in some less significant CIs. The size of the relevant units should be evaluated in conjunction with the better experience dissipation and enhanced ways to process information, as well as the economies of scale, achieved by the significant concentration of the banking sector during the last five years.
- c) All CIs submit on a semiannual and annual basis particular reports and data, for the purposes of supervisory assessment conducted by the Bank of Greece, including AML policies and procedures, important measures taken during the last year, description of AML IT systems, training courses undertaken, summarized inspection reports conducted by Internal Audit Unit and the AML Officer, including identified weaknesses, number of STRs submitted to AML Officer and to FIU, corrective measures / initiatives scheduled for the next year. Also, according to Governor's Act 2651/2012, CIs report, semi-annually through a standardized form, quantitative data concerning high risk customers and transactions (e.g. deposits and loans of offshore companies, PEPs etc.), which form the basis for the supervisory assessment of the CI's risk profile (details in the relevant variable for the effectiveness of supervision procedures and practices).
- d) IT infrastructure plays an essential role in the effectiveness of the compliance function. IT systems conduct the assessment of customers' risk and the monitoring of their transactions (including screening against sanctions lists), in a risk based manner, assisting the Compliance Unit to focus on the detection and management of high risk transactions (unusual/ suspicious ones) and customers. IT systems also allow for the accomplishment of off-site audits, on behalf of the Compliance Unit, in accordance with par. 9.2 of Decision 281/2009, with respect to the monitoring of the effectiveness of AML procedures and policies.

- e) The Compliance Units of the four significant CIs conducted, on average, 150-200 on-site and off-site inspections, per year from 2014 to 2016. At the same time, each AML unit proposed the termination of the business relationships with 30-50 customers, on average, per year. However, in some less significant CIs, IT systems had deficiencies in their parameterization, leading to a less effective monitoring of transactions. In these cases CIs have scheduled remedial processes, in order to handle deficiencies and improve operational capacity of the Compliance Unit in total.

4.4.1.9. AML knowledge of bank's staff

Assessment rating: Medium High

Systematic AML/CFT training is a significant requirement, according to the framework (Article 42 of Law 3691/2008, chapter 10 of Decision 281/2009).

Staff attends at regular intervals AML/CFT training programs, which are provided either through physical presence or through web applications. The training programs are usually organized by the training departments of credit institutions, often through collaboration with the Hellenic Banking Institute (hereinafter HBI)²¹⁹ of the Hellenic Bank Association (hereinafter HBA). Furthermore, CIs have processes for the assessment of their staff (e.g. self-assessment tests of the participants, questionnaires on the efficiency of training programs etc.)

For the period 2012-2016, there have been more than 60.000 participants in AML/CFT training programs, (including those working in the compliance units). For reference purposes only, the Banking Sector has as of 31.12.2016 approximately 43.000 employees. Moreover, the HBI has developed an interbank training system which covers, among other subjects, AML/CFT knowledge and skills. For the period 2014-2016, more than 10.000 persons (including those working in the compliance divisions) have been trained in AML/CFT issues by the HBI.

Although seminars addressed to compliance units' personnel are usually targeted to their specific AML/CFT responsibilities, the same does not always apply to the training of the rest of the personnel, responsible in operational activities. More particularly, AML training courses provided to front line or employees of specific units (large corporates' lending, private banking etc), often either lack specialization regarding the specific tasks and responsibilities of their operational assignment or focus heavily on procedural issues that are not adequately related to the ML/FT risks. Consequently, AML awareness achieved through the seminars is short term and theoretical. Considering the development of the regulatory framework towards the risk based approach, it is imperative for CIs to adjust their training programs and spread the AML/CFT culture and awareness from the Compliance Unit to the rest of the organization.

4.4.1.10. Effectiveness of suspicious activity monitoring and reporting

Assessment rating: Medium High

Decision 281/2009 requires the installation of a discrete AML IT system that at a minimum will support operationally: a) customers' risk assessment and classification according to their economic/transactional profile and other criteria set by the CI²²⁰, b) transactions monitoring with respect to customer's economic profile, the anticipated operation of the account and the typology of unusual/ suspicious transactions²²¹

²¹⁹ http://www.hba.gr/Eti/EN/default_en.asp.

²²⁰ CIs are obliged to classify customers in at least three different risk categories (low, moderate, high) taking into account the risk emanating from the customer's business activities, transactional behavior, products and services provided to the customer, the country of origin or destination of the funds etc.

²²¹ Banking and Credit Matters Committee no. 285/2009 cites an indicative (non- exhaustive) typology of unusual/ suspicious transactions that CIs should consider during parameterization of their IT system.

and c) customers and transactions screening against sanctions lists, both foreign (published by EU and UN's Security Committees) and domestic (published by FIU). Screening is performed in real time, during the commencing of the business relationship or the execution of a single transaction and periodically, regarding the entire client base, in order to take into account any updates of the lists. Moreover, IT systems are required to detect missing information in customer databases and support strict regulatory requirements for record keeping (for least five years after the end of the business relationship or the execution of the transaction).

Apart from the detection of persons and entities subject to restrictive measures, IT systems may also be utilized for the detection of customers characterized as Politically Exposed Persons (PEPs). According to par. 5.15.2 of Decision 281/2009 and article 2 of Law 3691/2008, CIs are required to apply Enhanced Due Diligence (EDD) measures against PEPs (domestic and foreign), including senior management approval for the commencement of the business relationship, verification of the origin of wealth and funds that the business relationship or transaction concerns etc. Large CIs, given the size, structure and complexity of their operations, rely on IT infrastructure in order to screen their clientele periodically against automatically updated PEP lists and filter their transactions, especially electronic credit transfers. On the other hand, less significant CIs haven't installed appropriate IT controls to effectuate automatic detection of PEPs and rely mostly on client declarations.

The significant concentration in the Banking Sector has led to technical economies of scale in terms of the IT infrastructure of merged CIs. Furthermore, it resulted in a better understanding of information needs and enhanced ways to process and utilize it, which led to improved IT system calibration regarding suspicious transactions monitoring.

CIs, including those that don't accept deposits (and, therefore, entail a lower ML risk) have installed AML IT systems for the continuous monitoring of customers and transactions. However, in some less significant CIs, IT systems have deficiencies in their parameterization, leading to a less effective monitoring of transactions. In these cases, CIs have scheduled remedial processes, in order to handle deficiencies and improve operational capacity of the Compliance Unit. In addition, during 2016, three out of four significant CIs received in total more than 22.000 requests for information from tax or judicial authorities. In order to address this challenge, banks have further enhanced their IT and record keeping systems to enable them to manage incoming requests in an effective and less time consuming way.

On average, half of the alerts produced by the system are handled and assessed by the AML department within 7 days and 80% of alerts are handled within 30 days. According to data provided by the Hellenic FIU, during the last five years, STRs submitted by CIs account, on average, approximately for 41% of total STRs of the financial sector, while the vast majority of STRs submitted to FIU is related to tax evasion. In the last two years, STRs and the supporting documentation are submitted electronically, through the upgraded secure platform of the FIU.

The quality of STRs has improved during the last three years, even though, deficiencies in the analysis and supporting documentation of the cases still remain. Bank of Greece and the Hellenic FIU co-organize ad hoc meetings with the AML reporting officers, targeting better and more effective cooperation, raising awareness and STRs quality. The development of a feedback process from the FIU to the CIs would contribute further to the improvement of the STR quality and their ability to identify suspicious transactions or activities. Feedback could involve reviews of specific cases reported, as well as strategic

analysis of overall risk-based conclusions (i.e. trends on suspicious activity typologies or high risk sectors, best practices etc.).

4.5. Product and service vulnerability

For the purpose of the NRA exercise, eleven products were selected for assessment. The products included have significant stock or transactional size, affecting considerably the economic activity (loans/deposits of natural and legal persons, credit cards, credit transfers, cheques), or are of particular nature (Private Banking, Trade Financing, Correspondent Banking, Safe Deposit Services) entailing increased inherent ML risk, according to FATF papers, as well as the SNRA report of the European Commission. The Inherent Product vulnerability variables relate to specific features of the particular products under analysis, such as the size, the client base profile, the use of agents, the use of cash, the cross-border use, investment/savings features etc. The Final product vulnerability also depends on the availability of additional AML controls that are specific to the particular product. The Vulnerability assessment of the banking products and services is presented in the following graph

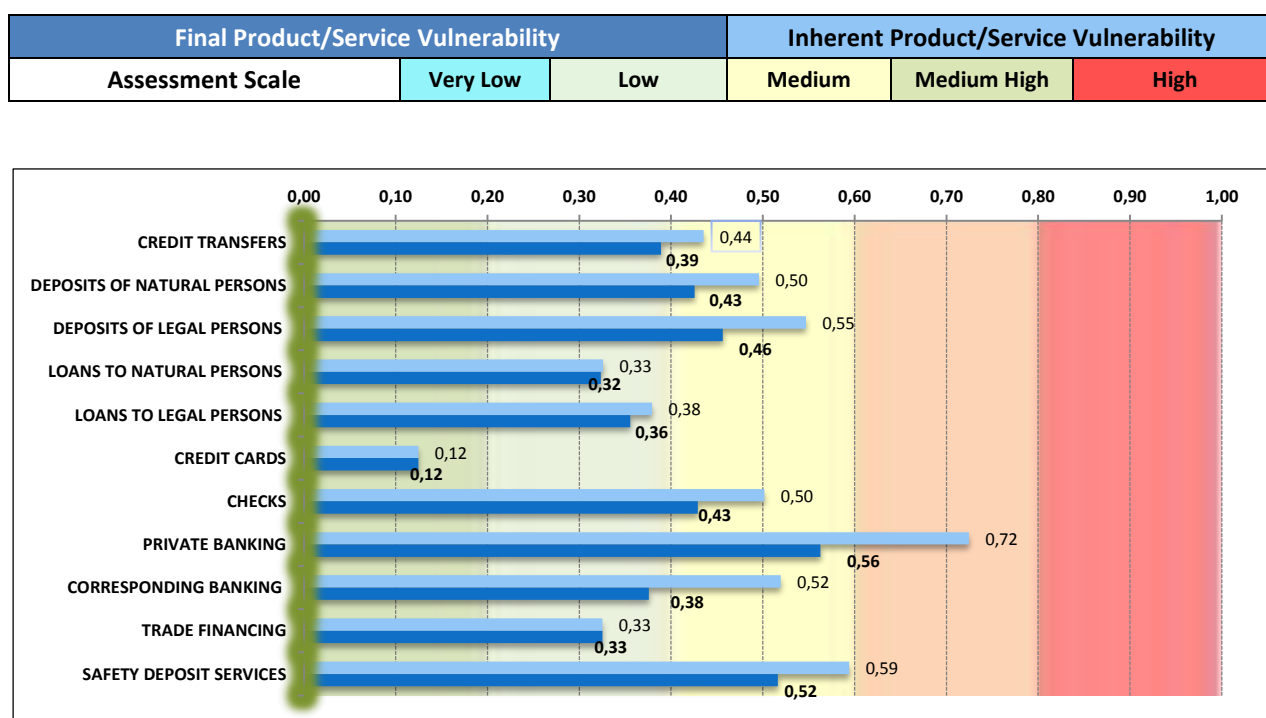


Table 33- Banking Sector : Final product/service vulnerability

The following paragraphs present in detail the rationale for the ratings assigned to the assessed banking products and services.

4.5.1. Deposits of natural persons

Assessment rating: Medium

As of 31 December 2016, the total value of deposits of natural persons (households, self-employed and sole proprietors) amounted to 99,257 billion euros, or 36% of total credit institutions' liabilities. Nevertheless, apart from the significant size, the rest of the assessment variables (cross-border transactions, cash activity, average transactions, client risk profiles) did not reveal material inherent ML

vulnerabilities and the overall transactions were within the expected retail parameters. Specifically: i) the total value of primary credits (“new money”) amounts to 125% of total deposits of natural persons, a relatively low ratio compared to legal persons (7 times higher), ii) the average primary deposit transaction size for the abovementioned time period amounted to 644 euros, iii) on an annual basis, the average active natural person receives primary credits close to the median income of the country (i.e. 7.520 euros in 2015), iv) only 2% of active clients are classified in high risk categories (PEPs, tax evasion and non-residents), holding 6% of the outstanding natural persons’ deposits, v) as expected for retail deposit accounts, the frequency of international transactions is limited, affected by capital controls imposed in July 2015, vi) the level of cash transactions in deposit accounts of natural persons is low, affected by the downward trend of cash deposits and withdrawals in the economy (approximately -50% since 2014 and -80% since 2012). The trend is mainly driven by the gradual application of administrative and regulatory framework that promotes the use of e-payments (e.g. credit transfers, direct debits, card payments) by consumers and firms, as well as capital controls.

The Final ML Vulnerability is assessed as “Medium” taking also into consideration:

- The operational characteristics of the product; account opening is always performed by physical presence of the customer, without the use of agents and omnibus use of deposit accounts is not available for natural persons.
- The adequate AML controls in place; customers are subject to stringent KYC procedures, which include a thorough review of the documentation provided, in accordance with the regulatory framework. This process is repeated after the expiry of the relevant documentation. Additional ML/TF controls exist for the high risk categories of PEPs, non-residents and self-employed, for which enhanced customer due diligence is applied, in accordance with the regulatory framework. The mandatory provision of the customer’s tax clearances sets the ground for the identification of unusual/suspicious transactions related mainly to tax evasion. Bank of Greece has also provided guidance for the proper calculation of primary credits into customers’ accounts in order to contribute to the proper identification of discrepancies in the customer’s transactions. Moreover, capital controls have introduced an additional due diligence process for certain categories of outgoing cross-border payments (tuition fees, hospitalization invoices for retail transactions exceeding a monthly limit of 1.000 euros).
- The fact that CIs have in general adequate core information systems that allow for transactions’ monitoring and recording. The concentration of the activity in the four significant CIs created subsequent economies of scale both in IT systems and applied AML controls. In addition, during the last 5 years when a significant banking consolidation took place, priority has been given to the data cleansing of customers’ databases. Finally, due to capital controls, credit institutions improved the transactional codes of their products/services, which allow them to monitor transactions more efficiently.

4.5.2. Deposits of legal persons

Assessment rating: Medium

Deposits of legal persons, although not very large in terms of outstanding value (25.359 billion euros as of 31/12/2016) have a significant volume and average size of transactions, as well as material cross-border and cash activity. Specifically: i) the average primary deposit transaction size amounted to 8.498 euros, which is 13 times higher than the average deposit transaction of natural persons (used as a benchmark), ii) 25% of total deposits are held by legal persons in specific high ML risk categories (e.g. off-shore

companies, NGOs, customers vulnerable to tax evasion) for which enhanced CDD is required, iii) cross border transactions (incoming and outgoing) of legal persons are significant (approximately 130 billion), albeit reduced from 2014 by at least -50%, due to the adverse economic conditions and capital controls, iv) cash deposits amount to 7% of primary debits of legal persons' accounts, while cash activity is affected by the downward trend of banking transactions in cash (as described in the product for natural persons).

The Final ML Vulnerability is assessed as "Medium". Corporate deposit accounts are related with numerous ML typologies, especially in the absence of a beneficial owner central registry. The ML risk is mitigated by the factors depicted in the Product "Deposits of Natural Persons" (lack of anonymity, lack of agents, advanced and recently updated IT monitoring / tracing systems) as well as:

- The fact that capital controls have introduced an additional due diligence process for certain categories of outgoing cross-border payments, allowing only those intended for documented business purposes (e.g. recent invoices due, supplier controls, ledger controls, thresholds based on history of cross-border transactions etc.).
- The use of omnibus deposit products is tiny (0,74% of total primary credits of the four (4) significant CIs), limited to certain categories of legal persons or financial institutions, such as insurance undertakings, e-money/payment institutions and investment firms that are also subject to the AML Law.

4.5.3. Credit transfers

Assessment rating: Medium

Credit Transfer is the most prominently used payment service, amounting, in 2016, to 79% of total payments of non-monetary financial institutions (hereinafter non-MFIs) with an increasing trend (2015: 75%, 2011: 73%). The total value of outgoing credit transfers of non MFIs amounted to 507 billion euros in 2016 (approx. three times the Greek GDP).

Credit transfers present similar inherent vulnerability characteristics to those of deposit accounts, in terms of average transaction, client risk profile and cross-border activity. Moreover, additional mitigating factors relevant for Deposits (lack of anonymous use, lack of agents, additional AML controls for customers entailing a higher risk of tax evasion and the imposition of capital controls, improved IT systems, etc.) are also applicable.

Consequently, the Final ML Vulnerability of Credit Transfers is assessed as "Medium", noting in addition the following:

- The large majority of credit transfers (68%) are performed in an automated manner, where the client provides the payment instructions in a standardized format (SEPA Credit Transfers).
- The number and the value of internet banking transactions have increased, on an annual basis, by 40% and 29% respectively, while the number and the value of mobile banking transactions have increased, on an annual basis, by 142% and 82% respectively.

CIs have taken, in recent years, extensive consumer and business awareness actions in order to protect payment service users from malicious actions. Consequently fraudulent transactions frequency is very limited (1 out of a total of 1,7 million transactions, and 1 euro out of 530 thousand euros).

4.5.4. Loans of natural and legal persons

Assessment rating: Medium Low

Loans towards the Private Sector (loans towards State and FIs were excluded), are significant in terms of size, presenting, as of 31/12/2016, an outstanding stock of 192 billion euros approximately, divided almost equally between legal and natural persons. Nevertheless, their importance as a funding source of the economy is diminishing due to the limited new funding (approximately 21 billions), consisting mostly of short term facilities to legal persons. Moreover, only 1,7% and 8,5% of total outstanding balances of loans, have been given, respectively, to natural and legal persons classified in high risk categories respectively.

Credit facilities are inherently vulnerable to operational risk, considering past incidents that led to severe legal or administrative sanctions for certain CIs (analytically described in section 2.1.6 above). Enhanced Internal Control Systems from an organizational, procedural and technological point of view are required for the management of Credit and Operational Risk entailed in loans, as well as the relevant ML vulnerabilities and typologies (cash collateral, early / significant reimbursements etc.). Considering that more than 44%²²² of credit facilities fall within “Non-Performing Exposures”²²³, the risks have shifted from new financing to loan restructurings. The recent measures that strengthened the organizational structure of the CIs and clarified the legal framework for the management of NPEs (i.e. the latest out-of-court debt settlement Law 4469/2017) are considered mitigating factors, in view of the targets for intensifying the management of the NPE stock in the following two years (2018-2019).

In addition, a number of AML/CFT controls, regarding TBML, KYC and CDD processes (including ultimate beneficial ownership), are supplemented by the Credit Controls applied before and after granting loans to legal persons, considering the current high level of NPLs and the decreased risk appetite.

Based on the above analysis, the Final ML vulnerability of Loans is assessed as Medium Low.

4.5.5. Cheques

Assessment rating: Medium

Cheques are payment instruments, authorizing the transfer of money from the deposit account of the issuer to deposit account of the beneficiary. Cheques have risk characteristics related to their prominent physical attributes that allow for anonymous or/and difficult to trace use (e.g. issuing as payable to bearer, post – dating and intermediary endorsements through hand-written signatures). Taking into consideration that Bank cheques are issued after the relevant amount has been withdrawn, the ML risk is mostly entailed in personal cheques, that are used as a credit instrument for business to business transactions and a substitute of a bill of exchange, providing guarantee for a payment on a future date (post-dated cheques). The combination of the above characteristics make the product attractive for ML through transferring money to counterparties without a legitimate business transaction or using collateralized post-dated cheques with fictitious or non-existent invoices.

Due to the vulnerability of the product, numerous ML typologies (15 scenarios) regarding cheques are included in the Decision 285/2009 of the Banking and Credit Committee of the Bank of Greece. Fraud

²²²Including off-balance sheet items. Excluding the off-balance sheet items and a current loan to the Greek State, which has been excluded from target-setting, the stock of NPEs is reduced by 2.6% in the second quarter of 2017 at €99.1 billion or 50.1% of total exposures.

²²³The European Banking Authority (EBA) definition on Non-Performing Exposures includes loans more than 90 days past due or loans whose debtor is assessed as unlikely to pay its credit obligations in full without realization of collateral, regardless of the existence of any past due amount or of the number of days past due.

cases have been identified in the past, related indicatively to falsification of the amount payable (ie Supreme Court Decision 567 / 2010), or the information on “blank” check bodies (Supreme Court Decision 1578 / 2010), or the intermediaries in order to manufacture “business relevance” between the issuer and the final bearer (Supreme Court Decision 225 / 2010).

The size of transactions, in terms of overall activity is 107,9 billion euros or 61% of GDP and the average payment is 19,7 and 12,5 thousand euros for bank and personal cheques respectively, higher than the average payment transaction (1000 euros). The majority of cheque payments are performed through personal cheques (60%), with indications of oversupply to the economy. At any given quarter of 2016, the number of unused personal cheques in circulation was approximately 13 million, while at the same period, the number of payments through personal cheques amounted to 5,3 million. On the other hand: i) cheque payments consist of 17% of total (non MFI) payments, with a downward year-to-year (-14,4%) and 5-year trend (26% of total non MFI payments in 2011), being gradually substituted by credit transfers, ii) the adverse economic conditions result in a gradual but consistent decrease in the demand for the product, as well as a decrease of the client base that is considered eligible for being granted personal cheque books, iii) the amount of unpaid personal checks has been reduced to a level of approximately 650 million euros (1% of the personal cheque payments), significantly lower compared to 2012 (1,3 billion euros) and 2009 (3 billion euros), iv) a limited amount of cheque transactions is performed by PEPs, non-residents and off-shore companies (0,7%), while 14% of payments are performed by clients entailing a high tax evasion risk, v) cross-border cheque payments are insignificant (0,2% of total).

The Final vulnerability of the product is assessed as Medium, considering also the following:

- Approximately 67% of cheque payments are interbank transactions settled through DIAS or the Athens Clearing Office. That strengthens the controls applied, as the required CDD is simultaneously applied by the CIs of the counterparties involved in the transactions.
- Due Diligence measures are applied by the CIs, based on the Decisions 281/2009 and 285/2009 of the Banking and Credit Committee of the Bank of Greece, for large / frequent transactions with cheques, based on their frequency, the length of period until the payment date, the number of endorsements, the consistency with the profile of the customers and the existence of personal or business relation between the beneficiary and the issuer (or last endorsee). Moreover, high risk clients involved in cheque transactions (approximately 15% of total) undergo Enhanced Due Diligence Measures (ie annual reassessment of ML risk of the client, tracing the source of funds, etc.).
- Clients depicted in the “black list” of Tiresias database of unpaid personal cheques or other administrative sanctions are not eligible for receiving new personal cheque books. Moreover, their existing stock of unused personal cheques cannot be used as collateral to short-term loans due to credit controls in place.
- Cheques are also affected by the capital control restrictions imposed in June 2015. Particularly the prohibition of cash withdrawals applies to all other cash payments by institutions, irrespective of currency, including redemption of cheques in cash.

4.5.6. Private banking

Assessment rating: Medium

Private Banking (PB) is defined as personalized financial and banking services that are offered to a bank's high net worth individual (HNWI) clients. The service entails higher ML risk, being attractive to ML perpetrators for a number of risk scenarios involving investments.

The Greek regulatory framework (par. 5.15.7 of Decision 281/2009) imposes enhanced customer due diligence measures for all clients receiving PB services.

As of 31/12/2016, the PB activity of the Banking Sector was concentrated in the four significant CIs, in approximately 27,6 thousand clients maintaining an investment portfolio of 7,1 billion euros. The PB service entails a material risk on an individual client basis, due to the significant average size of the transactions and portfolios (33 and 60 times larger than average respectively), related materially to cross-border investment stocks and flows (43% and 90% respectively).

There are also certain risk mitigating factors for consideration, such as the limited overall size and cash transactions, the concentration of the activity to significant Banks with better than average tracing systems and AML controls, the capital control restrictions that essentially forbid outgoing credit transfers for “old money” (money existed when capital controls were introduced) and the strict requirements of the regulatory framework, including those aimed to tackle tax evasion.

Based on the above, the Final ML vulnerability of the Private Banking Service is rated as Medium.

4.5.7. Trade financing

Assessment rating: Medium Low

Trade Financing is the financial component of an international trade transaction. According to relevant FATF documents regarding Trade Based ML (TBML), the ML vulnerability is concentrated in products such as letters of credit (L/Cs) and letters of guarantee (L/Gs), which provide the assurance of a CI that the underlying trade contracts will be honored. There is an increasing attractiveness of TBML as an alternative method of placement, that may be carried out in fictitious trade activities and/or through front companies, misrepresentation of the price, the quantity or the quality of imports or exports etc.

Nevertheless, the size of defaulted L/Gs (approximately 0,03 billion euros) and L/Cs issued in 2016 (0,77 billion euros) is insignificant and the risk profile of the counterparties involved in Trade Financing is low (only 2,6% are related to High Risk countries).

The Final ML vulnerability of Trade Financing is rated as Medium Low, taking also into consideration, the ML controls applied both on the clients and their counterparties (recorded in the IT systems of the CIs), and the lack of anonymity/ omnibus features. Moreover, detailed documentation and justification is required for cross-border outgoing credit transfers, according to capital controls legal framework, which constitutes a significant due diligence measure. The same rules apply to cross-border payments enabled by L/C, L/G products. Moreover, cross-border payments under L/C agreements are subject to controls regarding the trade financing documents. Finally, trade financing services do not provide anonymity or omnibus features, being available only to deposit customers.

4.5.8. Correspondent Banking

Assessment rating: Medium Low

Correspondent Banking is a “bank to bank” relationship where the correspondent processes transactions on behalf of the respondent’s customers, thus lacking an established business relationship and knowledge of their identity or the nature or purpose of the underlying transaction (unless this is included in the payment instruction).

The value of Correspondent Banking transactions, related only to the clients of the participant CIs is estimated at 50 billion euros approximately for 2016, which is significant, albeit with a downward trend

due to the establishment of payment systems for the settlement of domestic payments and the development of integrated euro payment systems.

Correspondent Banking entails increased ML risk, mainly in a 'nesting' scenario when the account is used on behalf of customers of other FIs (related to the respondent or belong to its Group), without the knowledge (and due diligence) of the correspondent, or when the service includes the opening of a payable-through account, which allows the respondent's customers to carry out transactions directly on the account of the respondent.

The above risk factors are largely mitigated considering the significant concentration of the activity to significant CIs (95% of Vostro transactions and 85% of Nostro transactions) and the low risk profile of correspondents and respondent CIs. Specifically, 89% of the Nostro transactions of significant CIs, are performed through correspondents that belong to the Wolfsburg Group, that require particularly high qualitative standards from their respondents and are considered to be a factor of "market pressure" (described analytically in the relevant General Variable). The rest of the correspondents are mainly Credit Institutions incorporated in European Union, USA, Canada and Australia. Moreover, 88% of Vostro transactions of significant CIs are performed by their cross-border subsidiaries or Branches.

The main weakness identified was the difficult and time-consuming traceability of the Correspondent Banking activity. The NRA exercise revealed that the CIs face difficulties in isolating the transactions related only to their clients and, even then, tackle the problem of multiple calculation of the same transaction.

Based on the above, the ML Vulnerability of Correspondent Banking is rated as Medium Low.

4.5.9. Safe deposit services

Assessment rating: Medium

Safe Deposit Services are provided in approximately 45% of the significant CIs' Branch network for the purpose of storing valuable possessions of their clientele. The content of a safe deposit box is not declared to the Credit Institution, while the access can be legally assigned to third natural persons. The service entails significant ML risk as a tool to escape tax or AML controls for hiding proceeds of crime that does not require specific expertise.

As of 31/12/2016, safe deposit contracts amounted to approximately 190 thousands (1% of active natural persons depositors), with a downward trend (-4% since 2015). Approximately 9% of clients using safe deposits were classified in High Risk categories, consisting mainly of Private Banking (37%), Tax Evasion (24%), HR Country relations (17%) and PEPs (2%). Moreover, 2% of safe deposit contracts were seized /frozen, due to restrictive measures imposed by tax and judicial authorities. In addition, during 2016, 14% of safe deposit boxes were accessed at least once by third assignees.

The attractiveness of the service is decreasing, considering the possibility of the issuance of seizing orders against Safe Deposits. According to article 46 of the Law 4174/2013, the tax authorities, in the context of taking preventing measures for safeguarding the public interest, are able to freeze at least 50% of the cash and 100% of non-cash items found in Safe Boxes of persons accused of crimes of tax evasion (above 150.000 euros).

Moreover, Safe deposit services are offered only to existing deposit clientele, and all CIs have client related as well as access-related AML typologies (access frequency, access from third parties etc.), according to the detailed AML Framework.

Based on above, the ML Vulnerability of Safe deposit services is rated as Medium.

4.5.10. Credit cards

Assessment rating: Low

A Credit Card is a payment instrument, regulated by the Payment Services Directive (2015/2366/EU). Credit cards enable cardholders to make purchases and/or withdraw cash up to a prearranged credit limit. The settlement occurs either in full by the end of a specified period, or in part, with the balance comprising a form of credit on which interest is usually charged (a revolving credit card). Interest usually begins one month after a purchase is made, and borrowing limits are pre-set according to the individual's credit rating.

The payments through Credit Cards issued in Greece are 4,9 billion euros, the average transaction size is 60 euros, cross border activity is 11% and cash repayments are 13% of total card repayments. Moreover, cash withdrawals via Credit Cards issued by local CIs were zero in 2016, due to capital controls.

The Final ML vulnerability of the product is Low, considering also that: i) issuing of anonymous cards is not allowed in Greece ii) non face to face use of the product/service is limited, as 86% of credit card transactions are performed at the Point of Sale and 14% are performed remotely, iii) fraud incidents are tiny (0,01%) and CIs have developed fraud-preventive methods/options (instant notifications per transaction, phone verification in unusual transactions etc.)

5. CAPITAL MARKET SECTOR

5.1. Overview

The Hellenic Capital Market Commission (HCMC) was established as a legal entity by Law 1969/91 and organized by Law 2324/1995, aiming to ensure the protection and the orderly and efficient operation of the Greek capital market.

The HCMC is a Member of the European Securities and Markets Authority (ESMA) and operates within its framework and under its auspices. HCMC is also a Member of the International Organization of Securities Commissions (IOSCO). HCMC concludes bilateral and multilateral agreements with other competent Authorities for the exchange of confidential information and cooperation in respect of issues relating to its competence.

It is responsible for the surveillance of the proper application of the regulatory framework to the Greek capital market. It participates decisively in the formation of the capital market regulatory framework, on a national, European and international level, contributing actively to the operations of the Council of the European Union, of ESMA and of IOSCO.

The HCMC supervises domestic and foreign firms offering investment services, fund and asset management firms and their products (UCITS, AIFs,) real estate investment trusts (REITS), companies listed in the Athens Stock Exchange in respect of transparency, corporate events, prospectuses in case of rights issues, financial statements, shareholders' obligations on notifications of changes in major holdings . HCMC also supervises the regulated markets, the clearing houses and investors' compensation schemes, such as the Guarantee Fund. It also observes the domestic and international developments, conducts research, when necessary, and certifies the professional suitability of market's participants. It receives and investigates investors' complaints.

HCMC also monitors and supervises transactions in respect of market abuse issues and actions of persons holding inside information.

It has the authority to impose administrative sanctions and measures, on natural and legal persons in violation of capital market legislation, and the authority to initiate criminal proceedings in cases where there are indications of serious criminal offenses in relation to the capital market framework.

It has an Anti-Money Laundering and Countering the Financing of Terrorism (AML/CFT) supervisory role over the institutions operating in the securities sector in Greece.

Finally, the HCMC has the responsibility to develop and enforce regulations regarding the compliance of the capital market with AML/CFT legislations and impose sanctions where necessary.

The entities under the supervision of the HCMC in relation to AML/CFT legislation are 57 Investment Services Firms, 15 Fund and Asset Management Companies, 2 Portfolio Investment Companies and 40 Receival and Transmission Companies.

- Investment Services Firms operate under MIFID and are licensed to trade in stocks, bonds, derivatives on behalf of clients and on their own account, and to act as investment advisers for corporate bodies and individuals.
- Fund and Asset Management Companies operate under UCITS (Undertakings for Collective Investments in Transferrable Securities) directive and AIFM (Alternative Investment Fund

Managers) directive and are licensed to manage UCITS and Alternative Investment Funds, and to offer discretionary asset management and investment advice as an ancillary service.

- Receival and Transmission Companies operate under national legislation and are licensed to receive and transmit investors' orders for both stocks and bonds.
- Portfolio Investment Companies operate under national legislation, are covered by the AIFM directive and are listed closed-end funds..

The Athens Exchange Group (ATHEX Group) operates the organised equities and derivatives market, the alternative market and performs clearing and settlement of trades. The ATHEX offers financing tools and solutions to companies, expands investor choice by providing a safe, stable and easy environment in full alignment with international practices and the European regulatory framework. The transactions carried out by the supervised entities are mainly exchange traded securities, bonds and derivatives, primarily on the Athens Stock Exchange.

	<i>Investor Accounts with balances</i>		<i>Capitalisation,</i>	
	<i>Number</i>	<i>Percentage (%)</i>	<i>Value (EUR million)</i>	<i>Percentage (%)</i>
<i>I. Domestic Investors</i>	<i>708,683</i>	<i>97.89</i>	<i>15,149.20</i>	<i>38.56</i>
<i>Private</i>	<i>702,533</i>	<i>97.04</i>	<i>5,831.38</i>	<i>14.84</i>
<i>Private financial firms</i>	<i>366</i>	<i>0.05</i>	<i>3,891.85</i>	<i>9.91</i>
<i>Private non-profit institutions</i>	<i>638</i>	<i>0.09</i>	<i>270.78</i>	<i>0.69</i>
<i>Non-financial firms</i>	<i>2,403</i>	<i>0.33</i>	<i>2,857.11</i>	<i>7.27</i>
<i>Public Sector</i>	<i>152</i>	<i>0.02</i>	<i>539.84</i>	<i>1.38</i>
<i>Other Investors</i>	<i>2,575</i>	<i>0.36</i>	<i>4.64</i>	<i>0.01</i>
<i>Hellenic Financial Stability Fund</i>	<i>1</i>	<i>0.00</i>	<i>1,753.58</i>	<i>4.46</i>
<i>II. Foreign Investors</i>	<i>14,982</i>	<i>2.07</i>	<i>24,120.32</i>	<i>61.40</i>
<i>Private</i>	<i>11,339</i>	<i>1.57</i>	<i>716.73</i>	<i>1.82</i>
<i>Private financial undertakings</i>	<i>2,724</i>	<i>0.38</i>	<i>17,039.89</i>	<i>43.37</i>
<i>Non-financial undertakings</i>	<i>799</i>	<i>0.11</i>	<i>5,233.69</i>	<i>13.32</i>
<i>Public Sector Organisations &</i>	<i>66</i>	<i>0.00</i>	<i>1,075.52</i>	<i>2.74</i>
<i>Other Investors</i>	<i>22</i>	<i>0.00</i>	<i>0.16</i>	<i>0.00</i>
<i>III. Other Investors</i>	<i>329</i>	<i>0.05</i>	<i>16.44</i>	<i>0.04</i>
<i>Total I + II + III</i>	<i>723,994</i>	<i>100.00</i>	<i>39,285.96</i>	<i>100.00</i>

Table 34- Capital Market Sector: Investor participation in the total capitalization of ATHEX, 2016

AML/CFT supervision conducted by the Hellenic Capital Market Commission is risk-based and in line with FATF's Risk-Based Approach for the Securities Sector, as well as the Risk-Based Supervision Guidelines issued by the European Supervisory Authorities.

The AML Supervisory Unit of the Hellenic Capital Market Commission counts 4 qualified examiners, with an auditing experience of at least 15 years in economics/finance with university postgraduate degrees,

computer skills and an excellent command of English. Considering the different sectors and the number of entities supervised by the Hellenic Capital Market Commission, as well as the range of its tasks and the upcoming changes in the regulatory framework, additional staffing would be appropriate (Supranational ML/TF Risk Assessment Report of the European Commission also puts emphasis on the need to build further supervisors' capacity in the EU). The type and the amount of administrative sanctions imposed both to the supervised entities and to senior management indicate their effective, proportionate and dissuasive nature.

5.2. Review of the capital market sector

The HCMC has the responsibility to develop and enforce AML/CFT regulations for the Capital Market. In this context, HCMC issues directives and guidelines, prepares typologies of suspicious behaviour, organizes training workshops for the prevention and suppression of money laundering and terrorist financing and carries out checks on supervised entities for the assessment of implemented procedures. For any deficiencies or violations found from these inspections, corrective measures or sanctions are imposed to the supervised entities.

The capital market sector has been subjected to a robust legal and regulatory AML/CFT framework²²⁴, which sets out detailed requirements with regard to customer identification and verification, record keeping, on-going monitoring and suspicious transactions reporting, internal controls, etc. Supervised entities are required to conduct the appropriate customer due diligence (CDD) measures and justify to the HCMC that the scope of the relevant measures is proportional to the ML/FT risk. The Effectiveness of Suspicious Activity Monitoring and Reporting is supported by specific AML IT systems which are established in some supervised entities (mainly the largest) and are required to conduct the basic operations of risk profiling, filtering transaction monitoring and sanctions, as well as the detection of PEPs.

It is important to note that the predominant way of accepting funds for placing investment orders to brokerage and other investment services providers is by bank deposits and bank transfers and that, therefore, transactions in cash in the capital market sector , are practically non-existent.

The main developments in the Greek capital market for the past five years include: the specific unfavorable market conditions which are related to the deep economic crisis, the imposition of heavy restrictions on capital movement in 2015 which includes increased KYC and restrictions on new bank account openings, as well as national legislation on transaction tracing and reporting. All the above create a framework that is totally unattractive to AML /CFT related fraudulent actions.

²²⁴See Annex for Capital Market Sector- Legal framework

<i>End of year</i>	<i>GDP In € Million</i>	<i>The Market Capitalisation of ATHEX Securities Market (€ million)</i>	<i>Number of ATHEX-listed companies</i>	<i>ATHEX market capitalisation (in% of GDP)</i>
2016	184,557	45,101.80*	207	25.6 %
2015	185,038	46,717.67	229	26.6 %
2014	185,685	52,916.45	233	29.7 %
2013	184,261	66,514.89	251	36.8 %
2012	190,289	33,766,01	265	17.7%

Table 35- Capital Market Sector: ATHEX cumulative data, 2012-2016

** The capitalization of table 34 differs from table 33 by an amount of €5,815.84 million because table 34 includes dual listed companies.*

Special mention should be made to the strengthening of capital market regulation, through both European and national legislation. Typical cases in point are the entry into application of Regulation EU No. 596/2014 on market abuse (MAR), which was accompanied by Law 4443/2016, the adoption of (national) legislation on equity crowdfunding, and various legislations on issues pertaining to bond loans (the reporting requirements for issuing corporations) and collective investments.

The total value of assets under management by the supervised entities stood at 10% in terms of the GDP, in December 2016.

<i>End of year</i>	<i>GDP in €mio</i>	<i>Funds under management (UCITS) in €mio</i>	<i>Portfolio investment companies in €mio</i>	<i>Assets under management in €mio</i>
2016	184,557	6,421	18	10,445

Table 36- Capital Market Sector: Assets under management, 2016

5.3. Capital market sector vulnerability assessment

Both vulnerability and threat of money laundering of the capital market sector result in the ML risk of the sector. The total vulnerability score of the capital market is graded as Medium (0.54), based on the analysis of the quality of the general AML controls and the inherent vulnerability of the capital market subsectors.

The approach used is the open-door approach.

The vulnerability of the securities sector regarding ML/TF derives from the products and services offered by the sector and other general factors such as the compliance function and supervision of supervised entities, enforcement of criminal sanctions, entry controls and the number of trained staff.

For the above assessment, we used quantitative and qualitative factors, including size of assets under management, value of transactions by product / security, assessment of training and AML knowledge of staff, size of the securities sector to GDP.

5.4. General AML controls

GENERAL INPUT VARIABLES		ASSESSMENT RATING
1	Comprehensiveness of AML Legal Framework	Very High
2	Effectiveness of Supervision Procedures and Practices	High
3	Availability and Enforcement of Administrative Sanctions	Very High
4	Availability and Enforcement of Criminal Sanctions	Medium
5	Availability and Effectiveness of Entry Controls	Medium High
6	Integrity of Staff in Securities Firms	Medium High
7	AML Knowledge of Staff in Securities Firms	High
8	Effectiveness of Compliance Function	High
9	Effectiveness of Suspicious Activity Monitoring and Reporting	Very High
10	Level of Market Pressure to Meet AML Standards	Close to excellent
11	Availability and Access to Beneficial Ownership Information	Medium
12	Availability of Reliable Infrastructure Identification	Medium
13	Availability of Independent Information Sources	Medium High
QUALITY OF GENERAL AML CONTROLS		Medium High

Table37- Capital Market Sector: Assessment of general AML controls

(The last three variables are analysed in the chapter of national vulnerability.)

From the analysis of the above variables, the quality of the general AML/CFT controls of the capital market sector is graded as Medium-High (0.66).

5.4.1. Comprehensiveness of AML legal framework

Assessment rating: Very High (0.8)

The European Directive 2005/60/EC has been fully incorporated through the Law 3691/2008. On top of that, FATF recommendations have been taken into account. Greece is in the process of incorporating the 4th AML Directive (EU) 2015/849 in its legal system. Supervised entities conduct the appropriate Customer Due Diligence using the risk-based approach (standard, simplified or enhanced), including

verification of the beneficial ownership of customers (whether it is natural persons, legal entities or legal arrangements). Additionally, Record-keeping, Enhanced Due Diligence for Politically Exposed Persons (PEPs) and high-risk countries, Reliance on Customer Due Diligence by third parties (including introduced business), Suspicious Transaction Reporting (STR), Tipping-off and confidentiality, Internal controls, foreign branches, and subsidiaries, Regulation and supervision of financial institutions, Supervisory powers, all have been provided for by the abovementioned law. Concerning, deposits and/or transfers to the supervised entities' bank accounts, no specific provision exists. Concerning the license (entry controls) required to operate, the following laws apply depending the type of entity: Investment Services Firm, Law 3606/2007 (Art.9-19); Fund and Asset Management Companies, Law 4099/2012 (Art. 12-19), [Alternative Investment Funds, Law 4209/2013 (Art. 6-11)]; Receival and Transmission companies, Law 3606/2007 (Art.36-40).

5.4.2. Effectiveness of supervision procedures and practices

Assessment rating: High (0.7)

Good understanding of the ML risk derives from the adequate experience and knowledge of the AML supervisory body staff. The HCMC has appropriate authority and mandate to conduct AML compliance supervision and it is clearly identified within the Law that it is in line with the European Directive and the FATF recommendations. On top of that, HCMC has issued its own rules and guidance on typologies.

Onsite inspections are performed on a risk based approach and have taken place for almost every supervised entity. Offsite inspections are performed based on reports submitted annually by all supervised institutions.

Year	Annual number of staff of AML supervisory body	Number of onsite inspections	(1) Total Fund and Asset Management Companies	(2) Total Investment Services Firms	(3) Total Receival and Transmission Companies	Total supervised entities (4)=(1+2+3)	% of total supervised entities inspected onsite
2016	4	19	15	57	40	112	17
2015	3.17	21	17	61	41	119	18
2014	2.67	27	16	63	51	130	21
2013	3.92	31	21	63	58	142	22
2012	3.08	22	19	64	65	148	15

Table 38- Capital Market Sector: Onsite audits

The assessment rating for this general variable is estimated as high because the number of trained staff is insufficient as described in the action plan. Considering the different sectors and the number of entities supervised by the HCMC, as well as the range of its tasks and the upcoming changes in the regulatory framework, additional staffing would be appropriate (Supranational ML/TF Risk Assessment Report of the European Commission also puts emphasis on the need to build further supervisors' capacity in the EU).

5.4.3. Availability and enforcement of administrative sanctions

Assessment rating: Very High (0.8)

Appropriate administrative sanctions are in place in Law 3691/2008 for noncompliance with AML obligations. They are also sufficient to influence positively management and staff behavior in securities

firms. There is a record of administrative enforcement actions taken in the past by HCMC regarding noncompliance with AML requirements in the assessed; institution types.

Year	Corrective measures imposed to number of Entities	Fines imposed
2016	1	20,000
2015	7	-
2014	5	-
2013	22	30,000
2012	3	25,000

Table 39- Capital Market Sector: Corrective measures and Fines imposed, 2012-2016

5.4.4. Availability and enforcement of criminal sanctions

Assessment rating: Medium (0.5)

Although Law 3691/2008 fully complies with the 3rd EU Directive and FATF recommendations and there is a record of Convictions and enforcement of criminal sanctions that have taken place over the past few years by HCMC for noncompliance with the Market abuse regulation in the assessed institution type, there is no conviction for ML. From 2002 to 2016, there are nine (9) cases of market abuse recorded, of which: two (2) of them are convicted, three (3) ended without conviction and the remaining four (4) are still pending. Based on the final court decisions these market abuse cases have not been linked for the enforcement of criminal sanctions on ML even though it is a predicate offence according to the law. Mediating measures on this weakness have been provided for in the action plan.

The assessment rating for this general variable is estimated as medium because of the lack of enforcement of criminal sanctions on ML.

5.4.5. Availability and enforcement of entry controls

Assessment rating: Medium High (0.6)

Entry controls are effective because they are clearly identified within the laws and regulations. For example: Investment Services Firms are licensed as per Law 3606/2007, Fund and Asset Management Companies are licensed as per Law 4099/2012 and Alternative Investment Fund Managers are licensed as per Law 4209/2013, Receival and Transmission companies are licensed as per Law 3606/2007 (Art.36-40). HCMC effectively carries out its licensing and entry controls duties. Thus, from 2012 up until 10/2/2017, there are 5 cases of no approval due to insufficient compliance with the HCMC requirements. Even though written AML internal procedures are required from the Licensee, this requirement is not specifically prescribed in law. The adequacy of these procedures is reviewed by the AML Special Unit.

The assessment rating for this general variable is medium high; an HCMC Decision on submitting written internal AML procedures is the key solution. (See action plan).

5.4.6. Integrity of staff in securities firms

Assessment rating: Medium High (0.6)

There is sufficient STR reporting to the FIU, thus the negligence or willful blindness is limited. The following table presents STRs submitted to the FIU.

YEAR	2012	2013	2014	2015	2016
INVESTMENT SERVICES FIRMS	36	41	47	51	41
FUND AND ASSET MANAGEMENT	31	18	9	26	9
RECEIVAL AND TRANSMISSION	0	0	0	0	0
PORTFOLIO INVESTMENT COS	0	0	0	0	0
Total	67	59	56	77	50

Table 40- Capital Market Sector: STRs submitted to FIU, 2012-2016

There are no appropriate mechanisms in place to protect securities firms staff against any negative consequences (pressure from firm's Shareholders or other staff) resulting from reporting STR, or other actions that comply with AML obligations. Relative decisions according to article 30 of law 3691 are not issued yet. Mediating measures on this drawback have been provided for in the action plan.

5.4.7. Integrity of staff in securities firms

Assessment rating: High (0.7)

Legislation requires the staff to be trained for AML issues. The awareness of the staff on AML compliance/procedures/obligations is being verified through the onsite inspections. 2015 Annual Reports state that: 50 % of compliance officers were trained, 50 % of supervised institutions trained their staff.

Investment Services Firms

Average number of staff per firm	Total staff	Total degree holders	Average number of AML Seminars for compliance officer	Av. Hours of training for compliance officer	Average number of AML Seminars for other staff	Av. number of participants for other staff	Av. Hours of training for other staff
21,72	1151	903	2,47	47,6	5,13	18,17	29,15

Table 41-Capital Market Sector: Staff training during 2012-2016

Fund and Asset Management

Average number of staff per firm	Total staff	Total degree holders	Average number of AML Seminars for compliance officer	Av. Hours of training for compliance officer	Average number of AML Seminars for other staff	Av. number of participants for other staff	Av. Hours of training for other staff
20,25	324	267	2,38	18,59	1,79	18,97	6,52

Table 42- Capital Market Sector: Staff training during 2012-2016

Receival and Transimission

Average number of staff per firm	Total staff	Total degree holders	Average number of AML Seminars for compliance officer	Av. Hours of training for compliance officer	Average number of AML Seminars for other staff	Av. number of participants for other staff	Av. Hours of training for other staff
3	89	70	2,79	7,21	2,17	4,9	4,38

Table 43- Capital Market Sector: Staff training during 2012-2016

5.4.8. Effectiveness of compliance function (organization)

Assessment rating: High (0.7)

The Law 3691/2008 article 41 requires firms to have adequate compliance programs. The adequacy of AML compliance/procedures is being verified through the onsite inspections.

An independent compliance officer is appointed at every firm except for very small firms with very low risk (Receival and Transmission) where the compliance officer is not independent.

A drawback to the function is that the bank statements for client deposits, kept by Investment Services Companies and Fund and Asset Management Companies, do not always show the actual depositor's name. Mediating measures on this drawback have been provided for in the action plan.

The assessed institution entities do take disciplinary actions against their staff for breaches of the compliance policy but they do not have a formal procedure for recording them. Formal recording procedure is not needed because of the small size of these companies and their nature (companies to a large extent family oriented).

According to HCMC Decision number 1/506/2009 article 9, every 3 years all supervised firms have to be audited by an independent auditor for their AML procedures.

5.4.9. Effectiveness of suspicious activity monitoring and reporting

Assessment rating: Very High (0.8)

Transactional records are available in a format that facilitates AML screening and monitoring. Securities firms have information systems that enable and facilitate the monitoring of client transactions against their profiles as verified by the on site audits as well as the answers received through the NRA questionnaires. Additionally, big securities firms are supported with systems performing effective PEP

screenings. The remaining medium and small size securities firms do not have such systems; they perform their PEP screenings based on personal relationships with their clients.

Through on site supervision, it has been verified that the securities firms are supported by systems which assist their staff effectively to: a) identify and record all complex, unusual large transactions and b) identify and report suspicious transactions. Finally, the staff has a good understanding of the scope of their reporting obligations on suspicious transactions and activities, including what activities are covered or not covered under laws. As it has been mentioned in paragraph 7 above, the staff has adequate AML knowledge.

In 2016, (see table 39), the number of STRs finally submitted to the FIU is considered reasonable, due to the fact that over 90% (INVESTMENT SERVICES FIRMS 93%, FUND AND ASSET MANAGEMENT 97.4%, RECEIVAL AND TRANSMISSION 86%) of securities accounts are not active, no new accounts are opened, the active customers are well known as they have a long term business relationship, the few new funds to be invested come to the investment firms through bank transfer or bank deposit and the volume and value of transactions has dropped dramatically.

5.4.10. Level of market pressure to meet AML standards

Assessment rating: Close to Excellent (0.9)

Based on the on site audits and the NRA questionnaire replies: a) the securities firms' have cross-border processing and settlement relationships that require compliance with international AML standards in order to maintain these relationships and b) the managements of the securities firms are sensitive to international and national AML-related reputational risks.

5.5. Inherent vulnerability variables

	Inherent Vulnerability	Final Vulnerability
INVESTMENT SERVICES FIRMS	0,68	0,54
FUND AND ASSET MANAGEMENT	0,27	0,27
RECEIVAL AND TRANSMISSION	0,16	0,16
PORTFOLIO INVESTMENTS COS	0,16	0,16

Table 44- Capital market Sector: Inherent Vulnerability

5.5.1. Investment services firms

Assessment rating: Medium High (0.68)

Reasoning for the given score: a) firms accept client funds and very rarely cash, b) the complexity and diversity of instruments offered is medium high, c) assets under management over the GDP is 6% (this percentage, based on the correlation of weight with the other sectors, is estimated as medium risk), d) in 2016, among other clients, firms have 135 PEPs, 1.054 off-shore companies, e) products are liquid, f) trade in stocks and bonds and are exposed to international transactions, g) may be exposed to market manipulation and h) insider trading and securities fraud.

Drawbacks, for which measures are provided in the action plan, are: a) Cash deposits are still feasible at Investment Services cashier, even though the majority of Investment Services Companies have abolished this mean of payment, b) Transfer of funds from customer's securities accounts to third party is still feasible, even though the majority of Investment Services Companies have abolished it, c) Through use of derivatives, possibility to transfer profits from one account to another. This is possible on the Athens Stock Exchange among others.

5.5.2. Fund and asset management companies

Assessment rating: Medium Low (0.27)

Reasoning for the given score: a) assets under management over the GDP are 4% (this percentage, based on the correlation of weight with the other sectors, is estimated as medium low risk), b) accept client funds into bank accounts only, c) the complexity and the diversity of products is low, d) the frequency of international transactions is low, e) in 2016, among other clients, firms have 253 PEPs, 36 off-shore companies and f) products are liquid.

5.5.3. Receival and transmission companies

Assessment rating: Low (0.16)

Reasoning for the given score: a) do not accept any client funds, b) the complexity is very low since they transmit orders for transactions in shares and bonds only, c) frequency of international transactions is low and d) in 2016, among other clients, firms have 3 PEPs.

5.5.4. Portfolio investment companies

Assessment rating: Low (0.16)

Reasoning for the given score: a) listed, closed-end fund companies, b) the complexity is very low and c) there is no differentiation concerning the risk factor compared to any other listed companies.

6. INSURANCE SECTOR

6.1. Summary

The Greek life insurance sector overall ML risk level was assessed as "Medium Low", which is determined by the ML threat level and the vulnerability level of the sector.

According to Chapter 3.4.2, concerning the evaluation of threat, life insurance products provided in Greek market do not offer enough flexibility and variety in order to be attractive to money launderers and require complex planning and knowledge from someone who want to launder money. Due to the above and in conjunction with the reduced involvement of the sector in ML cases, the level of threat was estimated as "Medium Low".

The assessment of insurance sector ML vulnerability, estimated as "Medium Low", was based on a detailed analysis conducted on both the quality of general AML Controls and the inherent/product specific vulnerability. The quality of General AML controls was assessed as marginally "Medium High" while the vulnerability level of Life Insurance products was generally assessed as "Medium Low", except for investment products assessed as "Medium".

6.2. Life insurance sector overview

Life insurance is a significant sector of private insurance activity, which generated premium income of € 1.9bn. in 2016, representing 50% of total insurance market in Greece (€3,8bill.), estimated at about to 1% of G.D.P.

As of October 2017 there were 22 life insurance companies in Greece (3 life only, 17 composite and 2 branches of EEA life insurance undertakings). The life insurance market has a high concentration ratio with the top 5 companies in 2016 in terms of premiums income accounted for 77% of the market and the top 10 companies accounting for 94%.

Life companies maintain very low cross border activity providing most of their business in the domestic Greek market. Although some of them are able to provide insurance products in other EEA Member States under the 'Freedom of Services' passport regime, the market share written abroad amounts to 1,59% of total life insurance premium income.

6.3. Insurance sector vulnerability assessment

The combination of insurance sector's vulnerability to money laundering and the money laundering threat to insurance sector determines the total money laundering risk to the sector. The Greek life insurance sector overall vulnerability was assessed as Medium Low, based on a detailed analysis conducted on both the quality of general AML Controls and the inherent/product specific vulnerability.

Insurance Sector Vulnerability	Medium Low (0.37/1.00)
---------------------------------------	-------------------------------

The overall vulnerability derives on the one hand, from the assessment of the quality of AML controls, which was assessed as marginally medium high ML/TF risk and on the other hand on the vulnerability of the insurance products analyzed, which in most cases was medium-low ML/TF risk except for investment products (particularly single premium) which was medium.

The analysis conducted on insurance product specific vulnerability took into account the most recent available, audited qualitative and quantitative data of the last 2-3 years, with the aim of better reflecting the most current risks in the insurance market. On the other hand, in the analysis of the general AML Controls and the vulnerabilities arising from them, the period of data collection was wider, reaching in some cases 10 years, depending on the assessed variable and the availability of statistics.

It is noted that this assessment considers only insurance companies that pursue life insurance activities (including investment products), since companies providing non-life and reinsurance activities are not designated as obliged persons under neither the Greek AML Law 3691/2008 nor the 3rd AML Directive and international AML Standards. According to the European Commission’s Supranational Risk Assessment report of June 2017, the level of ML threat related to non-life insurance is considered as lowly significant / non relevant.

6.4. General input variables

General input variables relate to the quality and effectiveness of general AML controls, and therefore apply to the entire insurance sector and affect the vulnerability of all the products being assessed. Higher ratings reduce the vulnerability of the insurance sector, while lower ratings increase the vulnerability of the insurance sector.

General Input Variables		Rating
1	Comprehensiveness of AML Legal Framework	High
2	Effectiveness of Supervision Procedures and Practices	Medium - High
3	Availability and Enforcement of Administrative Sanctions	High
4	Availability and Enforcement of Criminal Sanctions	High
5	Availability and Effectiveness of Entry Controls	Close to Excellent
6	Integrity of Staff in Insurance Companies	High
7	AML Knowledge of Staff in Insurance Companies	High
8	Effectiveness of Compliance Function (Organization)	Medium – High
9	Effectiveness of Suspicious Activity Monitoring and Reporting	Medium – High
10	Level of Market Pressure to Meet AML Standards	High
11	Availability and Access to Beneficial Ownership Information (analysis at national level)	Medium
12	Availability of Reliable Identification Infrastructure (analysis at national level)	Medium
13	Availability of Independent Information Sources (analysis at national level)	Medium – High
Total Assessment of General AML Controls		Medium - High

Table 45- Life insurance Sector - Evaluation of general AML controls

Based on the above analysis the Quality of General AML Controls is assessed as marginally Medium High.

Below is a brief analysis of the evaluation variables listed in the above table:

6.4.1. Comprehensiveness of AML legal framework

Assessment rating: High

The institutional framework for the prevention of ML is defined by the Greek AML Law 3691/5.8.2008 which transposes Directive 2005/60/EC of the European Parliament and the Council, and is specialized for insurance companies with Rule 154/2009 on “Prevention of the use of the financial system for money laundering and the financing of terrorism”, issued by the Hellenic Private Insurance Sector Committee (HPISC), which was the competent supervisory authority at the time of its issue. The current legal and regulatory framework is in line with the international standards regarding the application of customer due diligence (CDD) measures on a risk based approach (including customer and beneficial owner verification procedures, transaction monitoring procedures and IT systems), enhanced due diligence measures for several types of customers, products and delivery channels, such as PEPs, high risk countries, non-face to face transactions and use of new technologies. Proper provisions for Suspicious Transactions Reporting, internal controls, and record keeping are also included.

This assessment was based on Law 3691/2008 which was the legislation in force at the time of the first national risk assessment. Although the Directive (EU) 2015/849 had already been adopted it has not as yet been transposed in Greek legislation and therefore not considered in the analysis of the insurance sector vulnerability. However, the changes in the anti-money laundering framework brought about by the 4th AMLD were taken into account when defining the action plan to address the vulnerabilities and risks outlined.

Based on consultation with insurance companies and the supervisors, there are certain provisions of the current regulatory framework, which require further specification and interpretative guidelines in order to ensure a uniform and effective implementation by the insurance companies. These provisions include: a) the requirement for specialized IT systems that enable companies to effectively implement customer due diligence measures, including customer risk rating and monitoring of transactions based on typology of unusual/suspicious transactions, as provided by par.3, art 16 of Rule 154/2009 and b) the requirement for source of funds verification on customer payments exceeding €15.000, creates confusion in its implementation due to the absence of a common approach and definition on the time horizon to be checked in order to meet the above criterion when it comes to more than one transaction.

6.4.2. Availability and effectiveness of entry controls

Assessment rating: Close to Excellent

The Bank of Greece (BoG) is the supervisory authority for insurance companies and insurance intermediaries, since 2010, when according to Law 3867/03.08.2010 the Hellenic Private Insurance Supervisory Committee (HPISC) was abolished and all its responsibilities and powers, including AML supervision, were transferred to the BoG.

The prudential supervision is carried out by the Department of Private Insurance Supervision (DPIS), according to Law 4364/2016, which transposes Directive 2009/138/EC on the taking-up and pursuit of the business of Insurance and Reinsurance (Solvency II). The BoG has a clear and comprehensive framework for the licensing and registration requirements in the insurance sector. In particular, under Chapter B of Law 4364/2016, the BoG in addition to the capital requirements and the statutory purpose of the

applicant company, assesses whether the company a) is able to comply with the required Governance System, b) has written policies approved by the Board of Directors relating to risk management and internal controls and c) has fit and proper management and persons responsible for the company's key functions with appropriate educational and professional certification requirements. With respect to persons who have decided to acquire, directly or indirectly, a qualifying holding in an insurance or reinsurance undertaking based in Greece, according to Article 43 (para. 11), the Supervisory Authority, in order to ensure the sound and prudent administration of the (re)insurance undertaking to which the proposed acquisition relates and the likely influence of the proposed acquirer on that undertaking, it shall assess the suitability of the proposed acquirer and the economic assurances of the proposed acquirer, from a financial perspective, taking into account inter alia the extent to which there are reasonable grounds for suspecting that money laundering or terrorist financing is being committed, or attempted in connection with the proposed acquisition, within the meaning of Law 3691/2008 (A166) or whether the proposed acquisition may increase this risk.

The applicant companies, which due to their activity (life insurance) fall within the scope of AML Law, are also assessed for compliance with the existing institutional framework for the prevention of ML/TF by the competent AML Section of the BoG.

6.4.3. Effectiveness of supervision procedures and practices

Assessment rating: Medium High

The AML supervision of life insurance companies and insurance intermediaries is carried out by the AML Section of Supervised Institution Inspection Department (SIID) of the BoG, whose supervisory responsibilities are clearly defined in Article 6.3 of Law 3691/2008, ensuring the effective performance of its duties

The AML Section is responsible for the supervision of a number of financial institutions from different financial sectors including banks, life insurance companies, e-money institutions, payment institutions, leasing and factoring companies, credit companies, bureau de change, and Credit Servicing Firms. The total number of supervised entities as of October 2017 amount to 105. AML section conducts off-site and on-site supervision applying a risk based approach and is also responsible for the formulation of the AML regulatory framework of the financial institutions subject to its supervision.

As already analyzed in detail under banking sector vulnerability section²²⁵, the AML Section counts 9 qualified examiners, with a long audit experiences. However, given the wide range of duties of the AML Section and the upcoming challenges due to the modification of the AML Legal and regulatory framework in light of the 4th AMLD, it is important that the AML Section is further staffed.

The AML Section of the BoG defines its Supervisory Strategy, specifying the supervisory actions to be taken for each financial institution, including off-site and on-site inspections program along with the allocation of the available resources to the different financial sectors and financial institutions supervised by the BoG. The supervisory strategy is updated at least on a yearly basis and in the first place depends on the assessment of risks entailed in each of the supervised sectors and then on the assessment of individual financial institutions within these sectors. The sectorial risk assessment takes into consideration several factors such as the size of the sector, the number of entities within the sector and the level of

²²⁵ See section 4.4 of the Banking Sector Chapter

concentration of the sector's market in a limited number of entities, the level of complexity and increased risk of the products provided, the type and risk profile of customers they transact with, the level of compliance with current legal framework and the level of awareness of the sector etc. Based on this assessment BoG gives more emphasis and allocate more resources to the higher risk sectors.

AML Section performs an individual off-site risk assessment for each insurance company, as it does for every supervised institution and identifies ML risks pertaining to the insurance sector in general, based on data and information collected on a regular basis. Until recently, the offsite assessment for insurance companies, although quite robust, it was more focused on the control environment and the level of compliance of the insurance companies rather than on the inherent risk component for which a less detailed analysis was conducted. In this direction and in the context of the incorporation and implementation of the provisions of the 4th AML Directive and the new Greek AML Law, the AML section is currently in the process of finalizing a new risk based supervisory tool, in line with the principles set in the ESA's Guidelines on the Risk Based Supervision. The new risk based supervisory tool, aims at strengthening the risk component of the assessment and facilitates the efficient allocation of supervisory resources, taking into consideration the focus, depth, duration and frequency of on-site and off-site activities, supervisory staffing needs and technical expertise, commensurate to the level of money laundering and terrorist financing (ML/TF) risk associated with the financial institutions in the insurance sector.

On-site inspections are conducted according to the AML Section's Manual, which covers in detail all different areas of inspection. Since 2010, the BoG has conducted nineteen (19) on-site inspections in fourteen (14) life insurance companies. The companies inspected so far include the 5 largest (in terms of market share of total life insurance premium income), which were selected due to their risk and the size of their portfolios, while the rest, which are medium and lower size insurance companies, were selected due to other compliance assessment triggers (control environment issues). Despite the satisfactory level of compliance, the on-site inspections have identified weaknesses, which are summarized in the following areas: a) customer risk rating, b) transaction monitoring IT systems, c) insufficiently staffed AML units.

6.4.4. Availability and enforcement of administrative sanctions

Assessment rating:High

Obligated persons (legal entities and natural persons) under AML Law are subject to administrative sanctions in cases of non-compliance with their obligations under the provisions of the AML law, the relevant regulations and decisions of the European Union, the ministerial decisions and decisions of the FIU or the competent AML supervisory authority, as set out in art. 52 of the AML Law 3691/2008. The range of administrative sanctions which can be imposed by each supervisory authority is sufficiently broad to achieve the right balance between effectiveness, dissuasiveness and proportionality. In particular, it includes imposition of fines, corrective measures, removal of senior staff, temporary or permanent withdrawal of authorization or suspension of certain activities. The criteria applied by the BoG for the imposition of administrative sanctions to Insurance companies, are provided in art. 19 of Rule 154/2009 and include the risk that the violation in question poses in relation to money laundering and terrorist financing, the value of the illegal transactions carried out and the degree of the Company's participation, the level of possible economic benefits achieved, the level of Company's cooperation with the competent authorities and particularly with the BoG.

The BoG in the context of the above mentioned nineteen (19) AML on-site inspections conducted since 2010, depending on the significance of the findings and the risk involved, imposed a number of administrative sanctions including fines to five (5) insurance companies (amounting to €164.000) and corrective measures to six (6) insurance companies. In several cases where the findings were considered of low significance, no administrative sanctions were imposed rather corrective actions were requested in the course of offsite supervision.

The AML Section, in the course of its off-site supervision, checks the proper and timely implementation of the corrective measures imposed by the Credit and Insurance Matters Committee Decisions and conducts follow up inspections.

6.4.5. Availability and enforcement of criminal sanctions

Assessment rating: High

Dissuasive and proportional criminal sanctions for executives and employees of insurance companies due to non-compliance with AML/CFT obligations are in place, providing for imprisonment up to 10 years and fines up to €2mil., under AML Law (art. 45), as appropriate. There are no records of convictions and criminal enforcement actions taken over the last five (5) years against insurance companies and their executives or employees, for non-compliance with AML/CFT requirements. During the same period of the last five (5) years, the cases of integrity failure are also limited. Most of the detected cases were fraud cases (embezzlement, forgery) and involved intermediaries rather than insurance companies' employees. Where those cases involved employees of the company, the latter had fired them. Where intermediaries were involved, the company had terminated its cooperation with them and took legal actions against them. However, it is noted that there is difficulty to collect related data from the judicial authorities or public prosecutors, since criminal records are not categorized according to their offence and there are no statistical data for the years 2014-2016.

In the past and especially in the period 2007-2010, there were some criminal cases that have been filed against either insurance companies or their executive directors and employees, mainly for cases of deception of the insured persons. These cases concern companies of which the license has been revoked. By taking over the supervision of the insurance companies by the BoG and strengthening the supervisory framework by incorporating the Solvency II Directive (Law 4364/2016) in 2016, these incidents have been minimized.

6.4.6. Integrity of staff in insurance companies

Assessment rating: High

Insurance companies are required to comply with the "fit and proper" procedures provided by law 4364/2016, transposing Solvency II Directive. Bank of Greece performs fit and proper checks for the members of the board of directors, the beneficial owners and the persons who effectively control the undertaking as well as persons in charge of key functions, including the MLRO. The assessment is based on detailed questionnaires accompanied by relevant documentation. The Bank of Greece verifies the suitability and the reliability of the persons subject to notification requirements and informs the insurance and reinsurance undertaking, in case it has any objections.

Insurance companies have also developed Risk Management Systems for internal fraud, that apply to all staff members and include a) appropriate organizational structures, defining roles & responsibilities for all

staff members (4 eyes principle, written procedures, record keeping etc.), b) Policies & Procedures regarding staff vetting / identification, monitoring and reporting of internal fraud (Codes of Conduct, Conflict of Interest Policies, Recruitment Policies, Fraud Risk Management Policies, Irregular Behavior Reporting Policies, Whistleblowing Procedures, Anti - Bribery Policies etc.) c) Training programs / awareness raising of human resource d) Internal Control mechanisms and sanctions.

Based on information received from insurance companies for the period of the last 5 years, there were no cases of non-compliance with AML framework, involving insurance companies' staff. As regards cases of integrity failure in general, only 3 out of 20 insurance companies reported limited cases most of which involved intermediaries rather than insurance companies' employees. The cases reported mainly concerned fraud (embezzlement, forgery) and in all cases, the company had terminated its cooperation with the intermediaries involved.

6.4.7. Effectiveness of compliance function

Assessment rating: Medium High

Insurance Companies adopt AML policies and procedures, which are regularly updated in line with the current AML legal and regulatory framework, taking into account possible new risks that may occur over time. Under the existing framework the insurance companies' internal compliance programs are commensurate to the level of risk taking into account several factors such as the customer profile, the volume and the nature of products and transactions executed. In light of the new requirements of 4th AMLD, insurance companies should revise their compliance programs taking into account the ESA's Risk Factors Guidelines in order to be able to make informed, risk-based decisions on the effective management of individual business relationships and occasional transactions, based on an analytical and well-documented risk assessment.

Companies are required to nominate a fit and proper AML officer (AMLRO), who is responsible to ensure effective implementation of the AML policies and procedures, and the internal AML compliance program and functions at a senior level. The AML control mechanisms applied include AML audits performed by a) the Internal Audit Division according to their regular program b) the external auditors every 2 years and c) the AMLRO who performs specialized audits on a regular basis. In most companies the AMLRO duties are undertaken by the Head of Compliance Division, while in some cases are undertaken by the Head of Risk Management Division or the Head of Legal Department, ensuring to a large extent the lack of conflict of interest. The AMLRO is supported by additional properly trained personnel, in order to effectively perform his duties. According to information received by the companies and the supervisory authority, the number of staff employed in the AML units range from one (1) to three (3), depending on the size of the company. However in most of the cases the same people are also engaged with other equally demanding compliance duties, such as data protection, regulatory reporting etc. After taking into consideration factors such as the size of the individual companies, the nature and the volume of the products provided along with the level of automation of the AML IT systems, it was concluded that, insurance companies need to further increase the resources available to the AMLRO in order to be able to effectively perform his duties. Resource reinforcement concerns both staffing and IT systems support.

6.4.8. AML knowledge of staff in insurance companies

Assessment rating: High

Insurance companies are required to provide their staff with ongoing training in order to ensure that their knowledge of AML laws, policies, and procedures is appropriate and up-to-date. AMLROs regularly attend AML training programs and almost all of them have AML certifications. The level of AML knowledge of insurance companies' staff is considered satisfactory. Staff training program comprise of both in-company and external training programs, including e-learning seminars and regular informative circulars distributed to the staff along with the AML policies and procedures updates. Moreover, daily communication with the AMLRO and AML dedicated staff in the context of investigating unusual or suspicious transactions, substantially contributes to staff training (on the job training) and raises awareness. Through the above procedures staff becomes also aware of the legal consequences for non-compliance with their AML duties.

6.4.9. Level of market pressure to meet AML standards

Assessment rating: High

Most insurance companies are urged to meet international AML standards by market in one way or another. It is essential to note that according to recent survey, ten (10) life insurance companies, representing 89% of market share, replied that international market exert pressure on them to have an effective AML compliance function and they are evaluated for this purpose. In particular, a significant number of the life insurance companies operating in Greece are part of multinational Group of companies. In this context, parent companies require from their subsidiaries in Greece to comply with the international AML standards of the Group, especially in case where these standards are stricter than those provided by national law. In addition, parent companies systematically evaluate and monitor the level of compliance of their subsidiaries with the Group's AML Policy and require improvement measures if deemed necessary.

Furthermore, the effective implementation of the AML framework is also assessed by the foreign credit institutions where national insurance companies keep banking accounts, as well as by the cooperating reinsurance companies.

6.4.10. Effectiveness of suspicious activity monitoring and reporting

Assessment rating: Medium High

Insurance companies are required to maintain appropriate information technology (IT) systems, which enable and facilitate the monitoring of clients transactions against their economic profiles and assist them to effectively identify and record all complex, unusual large transactions. Most of the companies use specialized AML IT systems in order to detect unusual/suspicious transactions based on international typology while others, medium and low size companies, use specially designed regular and ad-hoc reports, targeted to high risk customers and high risk transactions. Sanctions screening and PEPs screening is mostly performed with the use of specialized AML IT systems or in-house IT solutions. Deficiencies identified by the BoG in the course of its supervisory actions (both off-site and on-site) with regard to the adequacy of IT systems that conduct suspicious activity monitoring and reporting refer to: a) failure to generate automatic alerts of unusual/suspicious transaction resulting in deficiencies with regard to effective justification of their assessment procedure from an auditor's point of view, b) insufficient

customer risk rating criteria which in several cases are more rule based and do not always incorporate a dynamic and ongoing assessment of the customer transaction activity and economic profile.

In the period 2014 – 2016, 1.507 STRs were submitted to the FIU by insurance companies. According to data received by the companies, 53% of the STRs filed were related to Investment products, 30% to Life insurance plans (death, survival, etc.) and 18% to Annuities products, indicating more or less the level of risk in each of the product category. None of these cases were referred to the prosecuting authorities by the FIU, while according to the latter, only 2 cases (STR's) reported back in 2010, were considered significant and were referred to justice. The abovementioned results of the FIU investigation on the STRs filed and the number of cases finally brought to justice, is an indication that the level of ML risk of the insurance sector is relatively low.

However, the FIU has identified some weaknesses with regard to the level of analysis and documentation of the STRs filed by life insurance companies. Another issue outlined by the FIU was the existence of “defensive reporting” in a significant scale since many of the STRs filed regard missing KYC documentation, regardless of the value of transactions. “Defensive reporting” mainly stems from companies concerns regarding the interpretation of the requirement to report suspicious transactions, as set out in the legal framework, especially for those possibly related to tax evasion.

6.4.11. Availability and access to beneficial ownership information

6.4.12. Availability of reliable identification infrastructure,

6.4.13. Availability of independent information sources

Assessment rating: Medium

Assessment rating: Medium

Assessment rating: Medium High

The last three vulnerability variables, which together define the quality of customer due diligence (CDD) framework, are assessed at a national level by both the National Vulnerability Group and the Banking Sector Vulnerability. The latter considers additional factors such as the institutional CDD framework and other additional control mechanisms applied by regulated financial institutions, including insurance firms. The quality of CDD Framework was collectively assessed as Medium (0.56) mainly due to lack of beneficial owners registry, at a national level. However, the lack of BO registry has no significant impact on life companies since life insurance products are predominantly held by individuals rather than companies.

6.5. Inherent vulnerability variables (Life insurance products analysis)

Inherent vulnerability variables relate to specific features of the particular products under analysis, such as the size of the product, the client base profile, the use of agents, the use of cash, the cross-border use of the product, investment/savings features etc.

Higher ratings increase the vulnerability of the product, thereby increasing the insurance sector vulnerability, while lower ratings decrease the insurance sector vulnerability.

The individual product vulnerability also depends on the availability of any additional AML control that is specific to that particular product. Specific AML controls (for certain products) have a similar impact as general AML control variables (higher ratings reduce the vulnerability of the insurance product; lower ratings increase the vulnerability of the insurance product)

The table below summarizes the final Inherent ML Vulnerability rating (product specific) as well as an indication of the size of each of product based on the premium allocation per class of insurance products in Greek market:

Life insurance product type/class	Market share (as of 2016)	Inherent ML vulnerability rating
Life insurance plans (death, survival, etc.)	36,5%	Medium Low
Annuities	5,2%	Medium Low
Pure protection & health/medical insurance	34,8%	Very Low
Investment products (index/unit-linked)	13,3%	Medium
Group pension	10,1%	Medium Low

Table 46- – Life insurance sector – Inherent vulnerability per life insurance product

Product Vulnerability / Market share 2016

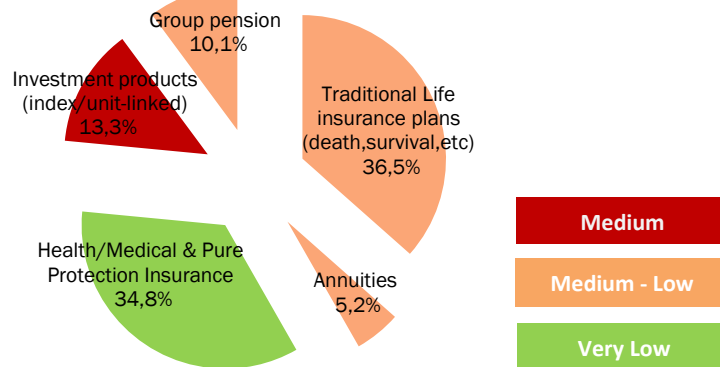


Table 47- Life insurance sector – Product vulnerability (market share 2016)

- Pure protection products pay their benefits on death or in respect of incapacity due to injury, sickness etc., while medical/health insurance products pay for the medical expenses of the insured person and are not even included in the scope of the Greek AML legal framework. Moreover, these two classes of products do not acquire a surrender value and the average annual premium paid is very low. Due to their nature and characteristics, pure protection and medical/health insurance

products are considered to entail very low ML risk and were not further analyzed under this assessment.

- Life insurance plans which provide coverage in the event of death of the life insured, and normally pay out on the death of the insured or earlier at a predetermined time in the future, are considered as medium low ML risk. Under this category, life insurance plans combine a death benefit with a savings component which can build cash value and they generally do not allow for extraordinary payments (top-up payments). For a long period of time after the policy initiation, usually lasting 6 to 7 years, the cash surrender value²²⁶ is significantly low compared to the premiums paid because of the high surrender charges²²⁷ that apply within that early period. In this respect the product is considered long term since the customer faces financial loss in case of early redemption, which in any case consists a typology of suspicious transaction and enhanced due diligence measures are applied accordingly.
- Annuities and group pension products, which offer an annuity with effect from a fixed date, related to the date of retirement or to a subsequent date, are considered medium low ML risk. The average premium paid is low while most of the products do not allow for extraordinary payments (top-up payments). By nature, individual and group pension products are considered long term. The low value of premiums contributed, combined with the surrender charges that apply during the first years (usually 3 to more than 5 years) of the insurance contract are dissuasive for policy holders to exercise early their surrender rights. In order to participate in a group pension product the existence of an active employment contract or relation with a company established in Greece is a precondition. Contributions are always linked to salaries, providing for maximum caps in the form of percentages on salary, while in case of premature surrender, the tax rates are increased by 50% as a means of penalty.
- Investment type products, which accumulate a financial benefit (unit linked, index linked etc.) for the policyholder at a future point in time and have a high cash surrender value, are considered as medium ML risk. The average annual premium is generally higher than in other insurance products and given their investment characteristics as well as their sophisticated terms and features, they may be more attractive to potential money launderers than protection or pension policies. Regular premium-investment products entail high surrender charges and administrative costs (deducted from the premiums paid and invested), especially during the first years of the investment. Particularly, in the first 3 years of the investment either there is no surrender value or the surrender penalties may range between 30-50% on the premiums paid so far. Therefore, the longer the investment period, the lower the surrender charges and administrative costs and in this respect, regular premium investment products are considered long term since the time horizon that usually yields return on the savings of the insured, is approximately 7 to 10 years. On the other hand, single premium investment products as well as option of extraordinary payments of regular premium investment products are the only ones that entail significantly lower surrender charges even in short term (usually 5%, 4% and 3% the first three years) and higher invested amounts (95-97% of premiums paid) and in this respect are considered to entail higher risk than regular premium products. The latter justifies the overall categorization of this type of products to medium risk.

²²⁶ Cash surrender value is the sum of money an insurance company pays to the policyholder in the event his policy is voluntarily terminated before its maturity or the insured event occurs.

²²⁷ Surrender charge is a fee levied on a life insurance policyholder upon cancellation of his or her life insurance policy, which is used to cover the costs of keeping the insurance policy on the insurance provider's books.

Final product /Service vulnerability	Inherent product/Service vulnerability				
Assessment scale	Very Low	Low	Medium	Medium High	High

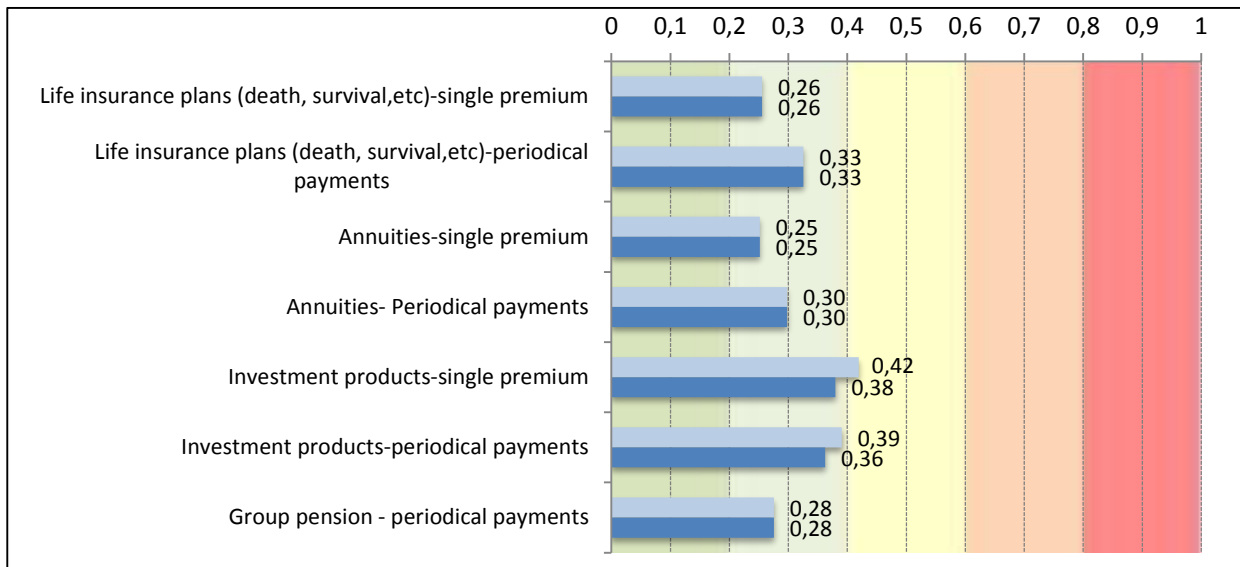


Table 48- Life insurance sector – Inherent vulnerability level per product

Besides the above product specific inherent vulnerability analysis, a horizontal analysis of some significant inherent vulnerability variables is provided below:

6.5.1. Use of intermediaries

The channels used by insurance companies to distribute their products beside direct sales, include banks (bank assurance) and intermediaries who for the purpose of this assessment with regard to ML vulnerability considerations, are split into two broad categories: i) the insurance intermediaries, who conclude exclusive cooperation agreements with a specific life insurance company (including “tied” intermediaries) and ii) those who do not conclude exclusive cooperation agreement any one company but provide the products of a number of life insurers. In circumstances where the life company use intermediaries for the collection of customer due diligence documentation and information, the last category (non-exclusive cooperation intermediaries) entail higher risk since exclusive cooperation intermediaries are better and more closely controlled by the companies. In particular they participate more often in company training programs and maintain a closer contact with its executives in general. A prerequisite for the lawful pursuit of the activity of an insurance intermediary is his/her registration with the Chamber of Commerce, meeting specific requirements, indicated in Art.4 of the Presidential Decree 190/2006 which include inter alia professional qualifications, CVs and experience certificates, criminal records, non-bankruptcy certificate, insurance coverage of their professional liability, etc. In addition, a certificate of successful exam tests which is being cared for by the BoG and which inter alia check their knowledge on the AML/CFT. The framework also requires that the holders attend follow-up seminars at least every five years in order to keep their certification up to date.

In 2016 life insurance products were mainly distributed through banks (36% of market share) and intermediaries with exclusive cooperation (39% of market share). The life products distributed through non-exclusive cooperation intermediaries amounted to 15% of market share and if health/medical insurance is excluded, only 7% of the markets share remains. In this respect, the ML risk related to the use of non-exclusive insurance intermediaries is significantly mitigated. In general, risk stemming from the use of intermediaries is mitigated also by the fact that intermediaries of life insurance products themselves are obliged persons under Greek AML Law. On top of this, insurance intermediaries are bound by the contract they conclude with the life company regarding the application of the AML policies and procedures and the due diligence measures in particular. Nevertheless, life insurance companies rely on their intermediaries only for the collection of KYC documents, which in any case, and always before customer initiation, are taken and checked by the company's back office employees who serve as the first line of defense.

6.5.2. Cash activity and tax evasion

Life insurance sector is not a cash intensive business. Most companies do not accept cash payments at all, while those that they do, they apply the upper limit of €500 in cash, as provided by law (par.3 art.20 of Law 3842/2010). Most of the companies expressly forbid the co-operating insurance intermediaries to collect premiums in cash except for some that allow for the first premium payment of new regular premium contracts only. Premium payments are made predominantly via electronic fund transfers or deposited in cash (for low value transactions) in the insurance companies' bank account.

Insurance products are not considered attractive for tax evaders and the perpetrators of the other prevalent proceed generating predicate offences in Greece due to a number of factors, including a) low volume and value of cash transactions and an average annual premium of approximately €700, b) easily traceable transactions since they are conducted through the banking system, c) annual reporting by insurance companies to tax authorities, on information regarding the life insurance policies of the taxpayers and the amount of premiums paid in each reporting period, as provided by Decision 1033/2014 article 2, and d) collection of income tax declaration by life insurance companies in the course of applying customer due diligence measures and particularly in order to justify the source of funds contributed by the customer. However, it is highlighted that the FIU has received STRs, potentially related to tax evasion, from insurance companies and informed the competent tax authorities. Competent tax authorities on their turn carry out checks on the basis of the information received and subsequently provide feedback to FIU for their own actions.

6.5.3. Anonymous and non-face to face use of products

Financial institutions, including insurance companies must not keep secret, anonymous or identified-by number accounts, anonymous passbooks or accounts in fictitious names or without the full name of their holder, in accordance with the identity certification documents, as provisioned by art.15 of AML Law. In addition, Greek insurance companies do not provide products "on behalf of whom it belongs", which contain elements of anonymity, since the beneficiary of the product is not defined at contract conclusion. However, there are a limited number of contracts (5% of total market) in which the beneficiaries of the insurance product are not specifically named but determined according to their characteristics, usually as "legal heirs". If the insurance event occurs, the beneficiaries are identified by a notarial act and the

company verifies their identity in the course of CDD measures application, at the time of payout. Therefore, the risk associated with the anonymous use of insurance products is considered very low.

Non-face-to-face customer initiation or conclusion of insurance contracts is not available. As already mentioned the distribution channels used by Greek insurance companies for life products include direct sales, banks and cooperating intermediaries, which in any case entail personal contact with the customer.

From all the above, the risk posed by the anonymous and non-face-to-face use of insurance products in the Greek insurance sector is considered to be very low..

7. OTHER FINANCIAL INSTITUTIONS SECTOR

7.1. Executive summary

The Other Financial Institutions (Other FIs) hold a relatively small share in the Greek economy on the basis of the financial figures of the relevant sectors, namely the money remitters, the electronic money issuers, the bureaux de change, the factoring companies, the financial leasing companies and the credit companies.

The payments and e-money industry experienced a significant surge in Europe in the last years due to the use of new technologies (Fintech) for Internet and mobile use, creating challenges in relation to the prevention of ML, whereas the remaining sectors remained traditional in their mode of operation. However, due to certain contextual factors linked to the Greek economic crisis, the respective sectors did not experience the same growth in the domestic market. In particular, the capital controls imposed in Greece in July 2015 had a significant impact on these markets as they imposed severe restrictions on outgoing cross-border remittances at client and company level as well as on cash withdrawals with pre-paid payment instruments. Moreover, the entry into force in March 2017 of Law 4446/2016 prohibiting the issuance of anonymous pre-paid payment instruments has a significant impact on the operation of the e-money sector, along with a mitigating effect in terms of ML risk.

In general, the total risk of ML of each sector is assessed as a combination of the ML threat and ML vulnerability, being "High" for money remitters, "Medium" for e-money issuers and bureaux de change, "Medium Low" for factoring companies and "Low" for financial leasing and credit companies.

Money remitters face the highest level of ML Threat (High) and ML Vulnerability (High Medium) among the Other FIs. Although the 20 money remitters operating in Greece conducted remittances of EUR 1.44 billion in 2016, which is quite low compared total country-wide payments, they experience vulnerabilities related to the widespread geographical provision of their services, the cash-based and cross-border nature of their transactions, false identification risk of their customers (mainly of refugees with less reliable identity documents) and the extensive use of agents. In addition, shortcomings were identified in the general AML controls, mainly related to the quality of Compliance Functions, the level of training of agents on AML issues and the quality of AML/CFT IT Systems.

The remaining five sectors do not seem to face particular levels of ML Threat. Regarding ML Vulnerability, e-money issuers and bureaux de change were assessed as "Medium", factoring companies as "Medium Low", while leasing and credit companies as "Low".

In particular, although only 4 electronic money issuers were operating in Greece in 2016 that issued electronic money of EUR 725 million, the assessment considered individual vulnerability factors related to the use of cash for charging pre-paid payment instruments distributed through extended networks of agents, as well as the remote conduct of transactions, of which a significant part is related to online gambling. The inherent vulnerability of the Sector is nevertheless mitigated by the AML controls in place and significantly by the prohibition of anonymity of pre-paid instruments that came into force in March 2017 through Law 4446/2016. The incorporation of the 4th AML Directive is expected to further mitigate the ML risk, as it imposes stricter provisions on simplified due diligence.

The 10 Bureaux de Change operating in Greece in 2016, exchanged banknotes of just 302,5 million euros. However, the nature of their cash-based activity may facilitate the ML process (at the placement stage),

given the inherent difficulties of monitoring occasional transactions that are usually lower than the threshold for the identification of the customer.

The ML risk is not adequately mitigated by the existing general AML controls, as weaknesses were identified in the licensing framework (outdated for a particular category of companies), the implementation of AML training programs, the quality of Compliance Functions and the parameterization of AML/CFT IT systems, in relation to (limited) typologies of suspicious transactions.

There are 5 Factoring companies operating in Greece with a turnover of 12,8 billion euros in 2016 and 8 Financial Leasing Companies with assets of 5,6 billion euros. The factoring and financial leasing activity in Greece is largely performed by subsidiaries of Credit Institutions with common corporate clientele, benefitting from synergies in operational processes (e.g. sales network) and AML Controls (e.g. Group Compliance Organization and Policies, information on ML risk assessment, transaction monitoring systems, common AML Training etc). Moreover, the credit nature of their services and the existence of product specific controls increase the quality of due diligence measures.

Finally, the lending activity of the 3 Credit Companies with an outstanding value of 372,2 million euros in 2016, has significantly declined in past years, while the AML controls in place are generally proportional to the limited risks and ML/TF typologies of the sector.

7.2. Other financial institutions ML vulnerability

Other FIs comprise of Money Remitters that provide retail transfers of funds, E-Money Issuers that provide money issuing, storage and payment services through digital wallets, Bureaux de Change that exchange foreign banknotes, Factoring and Financial Leasing Companies that address business financing needs and Credit Companies that provide small consumer loans or credit cards.

As presented in the Table below, the ML Vulnerability of each Sector is assessed based on the Inherent Vulnerability and the quality of the General AML Controls in place, analyzed synthetically according to the methodology provided by the World Bank.

	Money Remitters	E-Money Issuers	Bureaux de Change	Factoring Companies	Financial Leasing Companies	Credit Companies
Inherent Vulnerability	Medium High (0,74)	Medium (0,50)	Medium (0,38)	Medium Low (0,21)	Low (0,18)	Low (0,19)
General AML Controls	Medium Low	Medium	Medium Low	Medium High	Medium High	Medium
Overall ML Vulnerability	Medium High (0,68)	Medium (0,47)	Medium (0,40)	Medium Low (0,21)	Low (0,18)	Low (0,19)

Table 49- Other FIs: ML vulnerability

7.3. Inherent ML vulnerability

The Inherent Vulnerability of each Sector was assessed based on a synthetic analysis of several variables as depicted in the Table.

Inherent Variables	Money Remitters	E-Money Issuers	Bureaux de Change	Factoring Companies	Financial Leasing Companies	Credit Companies
Total Size/Volume	Medium Low	Low	Low	Medium High	Medium	Low
Client Base Profile	Medium Risk	Medium Risk	Medium Risk	Low	Low	Low
Use of Agents	Medium High	Medium High	Does not Exist	Does not Exist	Does not Exist	Does not Exist
Level of Cash Activity	High	Medium High	High	Does not Exist	Does not Exist	Medium Low
Frequency of International Transactions	High	Low	Does not Exist	Low	Low	Low
Anonymous use of the product	Not available	Available	Available	Not available	Not available	Not available
Difficulty in tracing the transaction records	Easy to Trace	Easy to Trace	Difficult/ Time Consuming	Easy to Trace	Easy to Trace	Easy to Trace
Existence of ML typologies on the abuse	Exist and Significant	Exist	Exist but Limited	Exist but Limited	Exist but Limited	Exist but Limited
Use in fraud or tax evasion schemes	Exist	Exist	Exist but Limited	Exist but Limited	Exist but Limited	Exist but Limited
Non face to face use of the product	Available but Limited	Available And Prominent	Not available	Not available	Not available	Available
Inherent ML Vulnerability	Medium High (0,74)	Medium (0,50)	Medium (0,38)	Medium Low (0,21)	Low (0,18)	Low (0,19)

Table 50- Other FIs: Inherent ML vulnerability

7.3.1. Money remitters

Assessment Rating: Medium –High

Money remitters provide a payment services without any payment account being created in the name of the payer or the payee. The services solely involve the transferring of the corresponding amount to a payee or to another payment service provider acting on behalf of the payee. Money remittances are performed through cash-to-bank and cash-to-cash transactions. Cash-to-bank refers to transactions where the payee receives the transferred amount of money in his/her bank account, while cash-to-cash where the money is received in cash.

The money remittance sector involves 20 companies and is highly concentrated (85% and 97% of transactions are performed by the three and the seven largest companies respectively). Nine money remitters are licensed and directly supervised by the Bank of Greece, while the rest are licensed and supervised by the competent authority of their home country and operate in Greece through a branch or (mostly) agents under an EU passporting regime. Nevertheless, the latter are required to nominate a

central contact point, responsible for the agents' compliance with the Greek AML/CFT framework the adherence of reporting obligations to the Bank of Greece.

Money Remittances are not very large in terms of value (1,44 billion euros in 2016), being also reduced by capital controls, which imposed limits on the outgoing cross border activity at the client (1.000 euros monthly limit) and company level (approximately 40% of former remittance activity). Nevertheless, money remitters are assessed as the most vulnerable Sector to ML (Medium High) among Other FIs, affected by the widespread geographical provision of their services, the cash-based and cross-border nature of transactions, customer risk profile and the extensive use of agents. In particular:

- Cross border remittances are approximately 56% of total remittances and typically involve immigrants' transactions that are either outgoing payments to the countries of origin or incoming payments from relatives residing in western countries. The main countries of destination of funds in 2016 were Georgia (18,9%), Philippines (8,8%) and China (8,8%). Respectively the main countries of origin of funds were Germany (19,1%), the United States of America (10,9%) and the United Kingdom (5,9%). 8% of total cross border remittances involved high risk countries (as designated by FATF, along with countries which deemed as not cooperative for tax purposes based on a Decision of the Ministry of Finance), sent mainly to Philippines, FYROM and Lebanon or received mainly from Iraq, Lebanon and Afghanistan.
- The use of agents is a dominant feature of the money remittance business model, as they carried 45,3% of transactions of 2016 in terms of value. The number of agents and their outlets in 2016 was more than 1.430 and 3.160 respectively, including four credit institutions with more than 760 outlets, 1 payment institution with 3 outlets and 8 bureaux de change with 24 outlets, while the rest of them run another business (i.e. grocery shops).
- Customers of money remitters are mainly economic immigrants living and working in Greece. Although the large majority of a considerable number of refugees or illegitimate immigrants, mainly from Syria, passed from Greece in 2015-2016 and ended up to other EU countries, those that remained in Greece have been an additional source of ML/TF risk for Money Remitters due to the customer identification challenges they pose.
- Money remitters are vulnerable to ML/TF typologies. In particular, according to FATF's report on "Money Laundering through Money Remittance and Currency Exchange Providers", a number of law enforcement investigations has revealed that money remittances are frequently used as a vehicle for laundering illicit proceeds. Laundered proceeds in such cases come primarily from drug trafficking, fraud, economic crimes, trafficking in human beings, smuggling of human beings theft and smuggling.
- The level of anonymity is very low, since all required information, which in any case includes the name of the payer and the payee, is recorded in the money remitters IT system and accompanies any transfer of funds, making transactions easy to trace. Customers are required to display their ID card (or passport) for any transaction and copies of their documents are kept by the money remitters.

Regarding Hawala operations, according to FATF's relevant report²²⁸: "they are used, in some jurisdictions by legitimate customers for reasons of geography, culture, and lack of banking access. They are also used by individuals and entities seeking to evade currency controls, tax obligations, and sanctions. They generally operate in areas with a high percentage of expatriate workers and are visible to members of

²²⁸ <http://www.fatf-gafi.org/publications/methodsandtrends/documents/role-hawalas-in-ml-tf.html>

that community.” However, Greece has a well-developed banking and payments infrastructure, to which immigrants that reside and work in Greece have access.

7.3.2. E-money issuers

Assessment Rating: Medium

E-money issuers provide payment and money storage services related to the issue and use of electronic money as defined under the second E-Money Directive (2009/110/EC). The business model and the entailed risks differ among e-money issuers. The key difference is the reloadable versus non-reloadable functionality of e-money instruments. Another distinction is the manner in which e-money is issued, varying among cash, transfers of funds or through payments cards. There is also the distinction of whether e-money transactions are performed within a closed-loop system that includes both consumers and merchants (“three-party scheme”), or the issuer establishes relationships only with consumers and provides them with access to third-party payment systems (such as Visa/Mastercard).

The E-Money Sector consisted of 4 companies (as of 31.12.2016), 1 licensed and directly supervised by the Bank of Greece as a Greek E-money Institution and 3 licensed by the competent authority of their home country and operating in Greece through agents/distributors under the EU passporting regime.

The size of the sector is considered low, as the total value of e-money issued in Greece in 2016 amounted to 725 million euros and is far from experiencing the growth of other European countries boosted by Fintech (mostly mobile wallets usually opened with innovative CDD solutions). The sector has been also affected by capital controls that, in addition to limitations on outgoing cross border activity, imposed a prohibition on cash withdrawals by prepaid cards or other forms of e-money instruments. The sector is highly concentrated, since the two largest companies in terms of value of transactions of 2016 accounted for approximately 94% of the market. The ML Vulnerability of E-money issuers was assessed as Medium taking also into consideration the following factors:

- Although some e-money products may, in certain circumstances, entail transactions where the identity of the customer has not been verified (41,2% of e-money issued in 2016), e-money issuers are in position to trace all kind of transactions, even those pertaining to prepaid vouchers (each voucher bears a unique code enabling e-money issuers to trace its history, such as the location of its distribution and the merchant to whom it was used). The prohibition of anonymous e-money products imposed in Greece in March 2017 (a provision that is much stricter than that of the 4th AMLD) rectifies this vulnerability as it mitigates the risk of anonymous use.
- A substantial percentage of e-money issued in 2016 (approximately 60%) was redeemed to gambling companies, either directly (at their e-wallets) or indirectly (through debit of prepaid vouchers of other customers), which are also subject to the provisions of the 4th AMLD.
- The percentage of cash to the e-money issued in 2016 was approximately 50,7%. However, with regard to the redemption of e-money, the respective percentage was very low (approximately 2,9%).
- 52,3% of the value of transactions of e-money issuers in 2016 was carried out through 31 agents/distributors with more than 20.760 outlets, which typically involve retail commercial businesses. However, in contrast to money remittance business, the agent’s role is limited to the distribution of prepaid instruments.

7.3.3. Bureaux de change

Assessment Rating: Medium

10 bureaux de change offer currency exchange services in Greece, 3 of which conducted 76% of total transactions of 2016. Apart from the licensed bureaux de change, there are numerous companies (approximately 900 spots) in remote touristic places, such as hotels, travel agencies and restaurants, which are granted special license from the Bank of Greece to buy foreign currency (small amounts), only in the context of servicing their own customers. The basic prerequisite is to be located in places where there is no branch of banks or bureaux de change.

The size of the sector is considered Low. The currency exchange transactions performed in 2016 by bureaux de change amounted to 302,5 million euros, while the transactions performed by the aforementioned retail companies are estimated to 130 to 160 million euros. In addition, bureaux de change are not allowed to engage agents and do not conduct non-face-to-face transactions.

Nevertheless, the ML Vulnerability of the sector was assessed as Medium, considering:

- the anonymity of the service, as for a significant part of transactions (47,64%) that are below €1.000 the name of the customer is neither verified nor recorded in IT systems;
- the consequent difficulty in tracing transactions performed by the same client;
- customer risks related to a considerable number of refugees or illegitimate immigrants, mainly from Syria, who passed from Greece in 2015-2016 and ended up to other EU countries and used bureaux de change to exchange their local currencies at their entrance in Greece in 2015-2016.

7.3.4. Factoring companies

Assessment Rating: Medium Low

Factoring consists of financial services addressed to business clients and mainly include management, collection and financing of short-term commercial receivables.

As of 2016, there were five factoring companies operating in Greece that performed a turnover of 12,8 billion euros (7,3% of GDP, close to EU average of 10%). The Factoring Sector is strongly related to the Banking Sector, as all Factoring companies (companies operating under Law N. 1905/1990) are subsidiaries of credit institutions with common, at large, clients. Factoring companies owned by the four significant credit institutions hold 96,5% of the market.

The Factoring Sector has a significant size in comparison to Other FIs, in turnover terms. Factoring activity can be connected mostly with Trade Based ML typologies (TBML), such as transactions of misrepresented value. The ML Vulnerability of the Sector was assessed as Medium Low, taking into consideration the following factors:

- I. The common clientele between Factoring companies and credit institutions reinforces the applied Due Diligence measures. Moreover, the companies do not use agents, taking advantage of the extended network of their parent banks as a point of contact and business relationship initiation with existing clients of CIs. It is noted that there is a line of communication between the AML Units of the Group regarding the ML risk of their common clients.
- II. The risk of TBML is mitigated by a number of credit related controls applied simultaneously to suppliers and buyers. In particular:

- Due to credit risk diversification strategies applied, the company is in a position to monitor the business profile of each supplier and each buyer with a number of different counterparties. Therefore, in a scenario of buyer/supplier collusion for ML through falsification of accounting books or price overestimation, the transactions between them are more likely to be traced as unusual/atypical in comparison.
 - 82% of Factoring turnover befalls in “Announced” category, therefore most receivables are announced to and confirmed by the buyer. The supplier sends to the buyers an “assignment notification”, informing them that the factoring company becomes the assignee of the Accounts Receivables and undertakes their management and collection. In case of international factoring, the simultaneous involvement of the correspondent factoring company also increases due diligence. The factoring company performs regularly reconciliation with the buyers of the amount of the Assigned Receivables, as well as the expected proceeds and closely monitors the adherence of the payment terms effected between the supplier and the buyers.
 - 60% of Factoring befalls in “Recourse” category, which allows the Factoring companies to request from the supplier to repay the financed amount, in case of debtor’s default. Consequently, the parallel assessment of the supplier's as well as the debtor’s creditworthiness also increases the quality of due diligence performed.
- III. Transactions are performed through deposit accounts held in credit institutions, subject to credit institution’s AML/CFT controls (CDD, monitoring, etc.). In addition, cash repayments are insignificant (0,1% of total claims) and indirect, always made through a deposit account maintained in the parent credit institution. Moreover, no difficulty is ascertained in tracing the transaction records, as there are sufficient record-keeping procedures in place. Consequently, anonymous or non-face-to-face use of the service is not possible. Also,, the companies maintain an increased level of control to the transactions performed such as disbursements, legal ownership of the underlying claims and (for announced category) incoming repayments, that are made to the company and released later to the client. Finally, 13% of the activity is related to cross-border transactions (97% of which befalls to exporting category), for services provided to significant corporate clients that maintain, at the same time, credit lines in the parent credit institutions.
- IV. 27,7% of the value of the assigned claims as of 31/12/2016 involved high risk clients. This is mostly due to a mandatory regulatory requirement applicable to companies with bearer shares, although they are typically large companies with transparent company structures..

7.3.5. Financial leasing companies

Assessment Rating: Low

In Financial leasing service, the provider company is the legal owner of the leased asset, and the lessee has operating control over it. As of 2016 there were eight financial leasing companies operating in Greece, with total assets amounting to 5,6 billion euros (3% of GDP). Seven of them, concentrating approximately 95% of the sector’s size and almost 100% of new business volumes, are subsidiaries of significant credit institutions, sharing for the most part a common clientele of corporate entities.

Despite the medium size of the financial leasing Sector, the ML vulnerability is assessed as Low, taking into consideration the following:

- I. The credit nature of the service and consequently the need for assessment of credit risk increase the quality of due diligence performed towards the client (credit bureau checks, beneficial owner check, supplier research, contact of the potential lessee prior to agreeing to finance an asset etc.), as well as the leased asset (independent evaluation of the market price and purchase confirmation through invoice and legal documents, periodic audit of the movable assets etc.) Moreover, the companies control the flow of the funds (payments are made directly to the suppliers' deposit accounts) as well as the ownership title of the leased assets.
- II. The concentration of the financial leasing activity to subsidiaries of systemic credit institutions and the existence of common clientele reinforce the applied Due Diligence measures. Companies do not use agents, taking advantage of the extended network of their parent banks as a point of contact and business relationship initiation with clients with already established CDD.
- III. Purchase and reimbursement transactions are performed through deposit accounts held in credit institutions, subject to the credit institution's ML/FT controls (CDD, monitoring, etc.) Moreover, no difficulty was ascertained in tracing the transaction records, as there are sufficient record keeping rules, systems and procedures in place. Consequently, anonymous or non-face-to-face use of the service is not possible. In addition, cash repayments are insignificant (0,1% of total claims) and indirect, always made to the lessor's deposit account in a Credit Institution.
- IV. All customers are Greek residents and cross-border transactions are rare (1-2%), concerning equipment purchases from foreign suppliers or second - hand asset sales to a cross-border buyer. In the latter case, due diligent measures are also applied for the buyer. Moreover, the leasing activity rarely involves assets maintained in other countries, for ease of tracking and controlling the asset as well as the ownership / title.
- V. 28% of the value of the lease contracts as of 31/12/2016 was related to high risk customers. This is mostly due to a mandatory regulatory requirement applicable to companies with bearer shares, although they are large companies with transparent company structures.

7.3.6. Credit companies

Assessment Rating: Low

Credit companies grant credit to individuals for consumer and personal needs through small loans or credit cards. There are three credit companies operating in Greece, one of which concentrates 80% of total outstanding debt and is a member of a Greek banking group.

The credit activity has significantly declined in the last years due to the financial crisis, and its inherent vulnerability in terms of size is considered "Low" (outstanding debt amounted to 372,2 million euros in 31/12/2016), while new credit production has been almost zero in the last 4 years, (i.e. 24 credit cards in 2016). Capital controls reduced further the vulnerability of their offered service, due to prohibition on cash withdrawals from credit cards.

The vulnerability of the Sector was assessed as "Low", considering also the credit nature of the offered services that increases the quality of due diligence performed towards the customers.

7.4. General AML Controls

The rating assigned to each particular general input variable is depicted in the following table. In order to avoid repetition, the analysis justifying each control variable covers all sectors, while sector-specific characteristics are provided, when necessary.

General Input Variables	Money Remitters	E-Money Issuers	Bureaux de change	Factoring Companies	Financial Leasing Companies	Credit Companies
1. Comprehensiveness of AML Legal Framework	Medium High	Medium High	Medium High	High	High	High
2. Effectiveness of Supervision / Activities	Medium High	Medium High	Medium High	Medium High	Medium High	Medium High
3. Availability /Enforcement of Administrative Sanctions	High	Medium High	Medium High	Medium High	Medium High	Medium High
4. Availability / Enforcement of Criminal Sanctions	Medium High	Medium High	Medium High	Medium High	Medium High	Medium High
5. Availability / Effectiveness of Entry Controls	Very High	Very High	Medium	Very High	Very High	Very High
6. Integrity of Business Institution Staff	Medium High	Medium High	Medium High	Very High	Very High	High
7. AML Knowledge of Business Institution Staff	Medium Low	Medium High	Medium Low	High	High	Medium High
8. Effectiveness of Compliance Function (Organization)	Medium	Medium High	Medium	High	High	Medium High
9. Effectiveness of Suspicious Activity Monitoring and Reporting	Medium	Medium	Medium Low	Medium	Medium	Medium
10. Availability and Access to Beneficial Ownership information	Medium	Medium	Medium	Medium	Medium	Medium
11. Availability of Reliable Identification Infrastructure	Medium High	Medium High	Medium High	Medium High	Medium High	Medium High

12. Availability of Independent Information Sources	Medium High	Medium High	Medium High	Medium High	Medium High	Medium High
Total AML Controls	Medium Low	Medium	Medium Low	Medium High	Medium High	Medium

* * The variables 10-12 are assessed in relevant Chapter of National Vulnerability

Table 51- Other FIs: General AML controls

7.4.1. Comprehensiveness of AML legal framework

Other FIs, are subject to a robust AML Legal and Regulatory Framework, based on Law 3691/5.8.2008 (AML Law) and Decision 281/5/17.3.2009, which is analyzed in detail in the Banking Sector Vulnerability Assessment. Regulation is supplemented by Decision 285/6/9.7.2009 of the Banking and Credit Committee of the Bank of Greece which includes, on top of general typologies, particular sections regarding sector specific typologies. It is worth noting that on top of the CDD requirements imposed in other EU/FATF countries, Other FIs are obliged to verify their customers' income through their latest tax clearance or tax declaration form, as part of standard CDD measures when a business relationship is initiated or when occasional transactions of 15.000 euros are conducted (included those considered to be linked). In addition, the applicable framework has become much stricter since March 2017, when a particular provision of law 4446/2016 prohibiting anonymity of prepaid instruments entered into effect (a provision stricter than 4th AMLD).

The entry into effect since the 26th of June 2017 of Regulation (EU) 2015/847 on information accompanying transfers of funds should also be highlighted, as an additional factor of a strengthened regulatory framework, particularly important for payments. Lastly, the draft law transposing the provisions of Directive (EU) 2015/849 which has been submitted to Parliament and is analyzed in the Banking Sector Vulnerability Assessment imposes stricter provisions regarding the application of simplified due diligence by e-money issuers.

Nevertheless, a large set of the current provisions of the AML regulatory framework are largely oriented towards the Banking Sector and apply on a proportionality basis to Other FIs. The application of the proportionality principle creates an ambiguity, mostly regarding the following:

- **Bureaux de Change:** For transactions below 1.000€, there is an ambiguity in the prudential and AML/CFT regulatory framework, regarding whether the entities are obliged to keep information records of the name and ID number of the customers. Currently, the sector does not record any information below this threshold, which undermines its ability to trace and identify "linked" transactions.
- **Money Remitters, E-money Issuers and Bureaux de Change:** Ambiguity regarding the identification criteria of "linked transactions" summing to the threshold of €15.000 and triggering the application of full CDD measures. The variety of the applied criteria (usually time-related) is significant (from one week to one year).

7.4.2. Effectiveness of supervision/oversight activities

AML/CFT supervision of Other FIs is assigned to the Bank of Greece by virtue of article 6.2 of Law 3691/2008 (AML Law). Based on the 10th follow-up report of FATF Greece has undertaken sufficient action to address the shortcomings related to former R23 (supervision) having reached a satisfactory level

of compliance. The effectiveness of supervision/oversight is analyzed in the Banking Sector Vulnerability Assessment.

The AML Section counts 9 qualified examiners, who regularly attend specialized seminars. Significant expertise and awareness is also gained through the participation of the Section in FATF and the AML Committee of the European Supervisory Authorities, especially regarding the recent developments on the Fintech and Regtech areas (innovative CDD solutions, mobile apps etc). Nevertheless, considering the different sectors and the number of entities supervised, as well as the variety of its tasks, the AML Section of the Bank of Greece needs additional staffing.

AML/CFT supervision of Other FIs is risk-based, as the focus and resources are targeted towards the sectors more vulnerable to ML/TF risk. In this respect the AML Section focuses mainly to money remitters' activity (both those established in Greece and in other EU countries) by receiving semi-annually, data gathering forms on the cross-border transfers of funds per country of origin and destination, aimed to capture Inherent ML risk. In addition priority is given on the assessment of AML controls implemented by the industry. In particular, the AML Section of the Bank of Greece assesses annually the quality of the Compliance Function and the adequacy of the AML/CFT procedures and IT controls, based on the analysis of annual reports of the AML/CFT Officers, Internal Audit reports, and (if available) reports on the Internal Control Systems by external auditors. Based on the above data, a total risk rating is assigned to each financial institution. These ratings are used to decide on the supervisory actions and the allocation of AML/CFT supervisory resources, including decisions about the focus, depth, duration and frequency of on-site and off-site activities. Nevertheless, the Bank of Greece intends to enrich the offsite assessment of the Other FIs, including additional risk parameters capturing the inherent vulnerabilities of each sector.

During the last eight years (2009-2016), 20 on-site inspections have been carried out on money remitters (14 on-site inspections, including four particular inspections on their agents), bureaux de change (five on-site inspections) and financial leasing companies (one on-site inspection), covering about 83%, 50% and 20% of each market respectively. The on-site inspections were mainly targeted to companies with a lower quality of AML/CFT controls, taking also into consideration their size.

7.4.3. Availability and enforcement of administrative sanctions

Other FIs are subject to the administrative sanctions set out in art. 52 of Law 3691/2008 (analyzed in the Banking Sector Vulnerability Assessment). The range of sanctions is sufficiently broad to achieve the right balance between effectiveness, dissuasiveness and proportionality, as it includes corrective measures, fines (both for the company and for the staff), removal of staff or suspension of certain activities.

In the last eight years (2009-2016), the fines imposed for violations of the AML/CFT regulatory framework amounted to 160.000 euros (120.000 euros to money remitters and 40.000 to Financial Leasing companies). In addition, corrective measures have been imposed to 4 bureaux de change companies and to 1 money remitter. The measures were commensurate to the findings identified in the relevant investigations, taking into account parameters like the size of the companies and cases of recidivism.

7.4.4. Availability and enforcement of criminal sanctions

The legal framework of criminal sanctions against employees or executives of Other FIs that are involved in ML/FT offences is specified in article 45 of the AML Law 3691/2008, while criminal sanctions are also applicable for ancillary offences to ML. The sanctions include fines (up to €1.500.000) or/and

imprisonment (up to 20 years). No cases of criminal sanctions against Other FIs or their staff have been identified.

7.4.5. Availability and effectiveness of entry controls

Access to the activities performed by Other FIs is subject to the licensing and supervisory remit of the Bank of Greece, on the basis of the particular legal and regulatory framework .

With regard to payment institutions (including money remitters), law 3862/2010 transposed Directive 2007/64/EC, whereas law 4021/2011 transposed Directive 2009/110/EC with regard to e-money institutions. Both Directives are of maximum harmonization, meaning that in general, the same terms and conditions apply for payment institutions and e-money institutions operating through branches/agents across Europe.

Particular fit and proper assessment is carried out by the Bank of Greece on any prospective agent of payment institutions and e-money institutions. The required documents/data that the agents are set out by the Bank of Greece Governor's Act 2628/30.9.2010 and the Bank of Greece Executive Committee Act 33/19.12.2013, respectively.

In cases of payment institutions and e-money institutions established in other EU member states, which intend to engage agents in Greece, the Bank of Greece (upon receipt of a respective notification from the supervisory authority of their country, in accordance with Article 25 of Directive 2007/64/EC) requires them to provide the same documents/data required for the agents of the Greek payment institutions and e-money institutions, respectively. Therefore, these agents undergo dual fitness and properness assessment (both by the supervisory authority of their country and the Bank of Greece) and are registered in a public registry. Moreover, the Bank of Greece Executive Committee Act 33/19.12.2013 requires from these payment institutions and e-money institutions to nominate a local contact point, who should reside in Greece and be in charge of the application of the local AML legal and regulatory framework.

Other FIs which apply for authorization should submit, inter alia, information about the AML Officer who intend to nominate, the AML/CFT policy and procedures including the KYC, record keeping, reporting, internal controls, information about the AML IT system which they intend to establish, etc. They should also submit particular questionnaires for their beneficial owners and shareholders, the members of the Board of Directors, Internal Auditor and key directors, including the AML Officer. The Bank of Greece is sufficiently supported by policies and procedures regarding management, evaluation and monitoring of authorization applications.

The licensing activity of the past 6 years is the following:

- One application for authorization of a money remitter has been rejected due to the fact that the source of funds of the shareholders could not be justified. Moreover, the Bank of Greece rejected the engagement or requested the removal of more than 164 money remitters' agents (either of Greek payment institutions or payment institutions established in other EU member states) out of 3.019 applications/notifications (namely 5,43%), due to the fact that they were not deemed "fit and proper".
- Two applications for authorization of e-money institution have been assessed by the Bank of Greece, both of which have been approved (though the latter very recently-end of 2017). In addition, the Bank of Greece rejected the engagement of 5 out of 42 agents/distributors of e-money institutions, due to the fact that they were not deemed "fit and proper".

- One application for authorization of a bureau de change was submitted in 2017, which was approved in the same year.
- No applications have been submitted for the authorization of factoring, financial leasing and credit companies.

In terms of the licensing regime, the following deficiency was identified:

Bureaux de Change: There is an outdated framework (Monetary Committee Decision 176/20.9.1977) regarding licensing of certain retail companies to buy small amounts of foreign currency, only in the context of servicing their customers. The activities of these companies, despite a material volume, are not sufficiently monitored.

In terms of Hawala operations, in order to be considered as a legal activity, they should be provided by companies licensed under law 3862/2010 (Directive 2007/64/EC) as payment institutions, subject, as a consequence, to the provisions of the AML Law.

7.4.6. Integrity of business/institution staff

According to the licensing framework, Other FIs which apply for authorization should submit, inter alia, questionnaires for their beneficial owners and shareholders, members of the Board of Directors and key function holders, including the AML Officer. The same requirements apply upon the replacement of any of the above persons.

The AML regulatory framework sets out that financial institutions should take appropriate measures to protect the AML Officer reporting unusual or suspicious transactions to the FIU, as well as their employees filing internal reports of their suspicions.

Furthermore, according to Decision 281/5/17.3.2009 of the Banking and Credit Committee (paragraph 12.3.3), the AML Officer shall assess the adequacy of any authorized agent in terms of AML/CTF training and knowledge prior to the commencement of their cooperation. As already described in the variable "Availability and Effectiveness of Entry Controls", payment institutions and e-money institutions should submit to the Bank of Greece specific documents/data regarding fitness and propriety of any agent. Nevertheless, the level of integrity of money remitters' and e-money issuers' staff and agents is deemed more uneven in comparison with other sectors whose business models are not based on agents. The reason is that there is a lack of homogeneity among agents, while the internal monitoring of agents' level of integrity at regular intervals (not only at the beginning of their relationship) is not an easy task, compared to the respective monitoring of staff's integrity.

Particular information regarding each sector follows below:

Money remitters: According to the information received from the sector, the vast majority of money remitters established in Greece (more than 93% in terms of value of transactions) adopts hiring practices that involve background checks. They also have code of conduct in place, for which all the staff become aware. The prerequisites for the recruitment of some firms involve for instance the non-conviction for any offence. During the last five years there have been no criminal cases against staff members or other relevant incidents reported. However, two employees were identified to have undertaken a suspicious activity. One of them was dismissed and the other one received a monetary fine by the money remitter. Moreover, there was a case of an agent who had been the subject of a police investigation and consequent law enforcement actions. The relationship with this agent was immediately terminated.

E-money Issuers: At least for the single e-money institution which is licensed in Greece, there are specific policies and procedures in place, which concern not only the recruitment but also the ongoing cooperation with its employees, including Code of Conduct, Whistleblowing policy etc. There have been no criminal cases against staff members or other relevant incidents reported. However, there was one case of an employee with irregular behavior, who was dismissed.

Bureaux de Change: According to the information received from the sector, bureaux de change adopt hiring practices which involve background checks. However, not all of them communicated adequate procedures in order to safeguard the integrity of their staff, arguing that they are small companies which can easily control these behaviors, without any sophisticated procedure. During the last five years no criminal cases against staff members or other relative incidents have been reported.

Factoring and Financial Leasing Companies: There are appropriate mechanisms in place to protect managers and staff against any negative consequence that results from reporting suspicious transactions, or other actions undertaken in order to comply with AML obligations. The companies of the above sectors have in place adequate procedures that promote integrity (i.e. the Group or company Code of Conduct, clean legal history checks as a prerequisite for recruitment, Conflict of Interest policies etc.). The history of integrity failure incidents (e.g., negligent or “willful blindness” to suspicious transactions) involving staff is zero. Both types of sectors are considered to be positively influenced by the fact that they are subsidiaries of credit institutions, sharing similar hiring and vetting policies, code of conduct etc.

Credit Companies: According to the information received from the sector, they have adopted hiring practices that involve background checks. They also have a code of conduct in place, for which all staff become aware. During the last five years there were no cases of illegal or irregular behavior of their staff.

7.4.7. AML knowledge of business/institution staff

The existing AML/CFT regulatory framework, namely article 42 of law 3691/2008 and paragraph 1.3 (vii) of Decision 281/5/17.3.2009 of the Banking and Credit Committee sets out that the obliged entities, including Other FIs, should take appropriate measures so that their management and staff are informed about the AML/CFT provisions, and ensure their participation in specialized AML/CFT training courses. Moreover, according to paragraph 12.3.3 of the above Decision, the AML Officers of money remitters and e-money issuers should assess the adequacy of their agents in terms of AML/CTF training and knowledge prior to the commencement of their cooperation.

The following deficiencies have been identified for the particular sectors:

Money remitters and E-money Issuers: Despite the fact that a large part of transactions is performed by agents, they are usually not included in the regular AML/CFT training programs that Other FIs provide to their staff. Nevertheless, it should be noted that the type of transactions that agents/distributors of e-money institutions conduct in Greece (distribution of prepaid vouchers and loading of existing e-wallets) entails in general lower ML/TF risk than those carried out by agents of money remitters. Moreover, the agents of e-money issuers do not collect the customers’ KYC documents (this is normally done directly by the principal e-money issuer).

Bureaux de Change: Approximately 40% of the sector (in terms of value of transactions) did not perform sufficient AML training programs).

7.4.8. Effectiveness of compliance function (Organization)

Other FIs operate under a robust regulatory framework regarding Corporate Governance and Internal Control Systems, applied under the principle of proportionality and supervised by the Bank of Greece.

Based on the information received, a compliance function is established in all Other FIs, operating according to written AML Policies and Procedures. Nevertheless, at an organizational level, the quality of the Compliance Functions varies among different sectors.

The following deficiencies have been identified for the particular sectors:

Money Remitters: In general, the number of staff assigned to the AML/CFT functions (one to three persons) does not sufficiently take into account the overall risk of the sector, the volume and frequency of the transactions and, in some cases, the number of suspicious transactions' alerts that require "real-time" assessment. In addition, in few cases, the AML officers have additional operational responsibilities within the firm. Moreover, according to the experience from offsite and onsite inspections, several money remitters have AML/CFT manuals which do not explicitly describe all the range of the procedures applied and are not deemed comprehensive enough. Finally, although there are Internal Audit functions in place, the majority of their audits have a limited AML scope (KYC documents collected by the cashiers and the agents) and do not assess the core activities of the compliance functions (quality of alert management and assessment, adequacy of AML Policy, etc.).

Bureaux de Change: Most of AML/CFT manuals in place are not updated or/and describe poorly or partially the range of applied procedures. Moreover, most annual reports communicated to the Bank of Greece have deficiencies (i.e. IT description, scope of internal audits performed etc.).

7.4.9. Effectiveness of suspicious activity monitoring and reporting

Decision 281/5/17.3.2009 of the Banking and Credit Committee requires from Other FIs to install AML IT systems that will be perform a continuous monitoring and detection of suspicious or unusual transactions. In particular, par. 12.3.5 of Decision 281/2009 determines the minimum operational functions of a proper AML IT system. These functions are: 1) transactions monitoring on the basis of the international typology of suspicious transactions and issuing alerts of unusual or suspicious transactions and 2) customers and transactions screening against sanctions lists. Screening should be performed in real time, during the commencement of the execution of a single transaction and periodically, regarding the entire client base, in order to take into account any updates of the lists. Decision 285/6/9.7.2009 of the Banking and Credit Committee of the Bank of Greece includes, on top of general typologies, a particular section regarding sector specific typologies. It also includes typologies for the detection of Hawala, such as: "There is evidence of illegal/alternative money remittance mechanisms (hawala), e.g. large remittances by shop-owners not justified by their business activity, in particular in areas with strong presence of immigrants".

The following deficiencies were identified in some particular sectors:

Money Remitters: AML IT systems in place lack sufficient parameterization for identifying complex and sophisticated scenarios of unusual/suspicious transactions. Moreover, certain deficiencies have been identified through on-site investigations regarding monitoring of multiple transactions. In many cases, the monitoring process is not organized in a secure and efficient way (lack of audit trail, paper-based assessment procedures etc.) and relies heavily on under-staffed AML Units that are required to assess fast (before the transaction) a significant number of alerts of unusual transactions.

E-Money Issuers: There is a challenge to identify combined transactions of customers who use multiple e-money products and their transactions fall under the simplified due diligence measures, namely their identity is not verified. However, in view of the forthcoming new AML law, the leeway of simplified due diligence is going to be restricted to a great extent.

Bureaux de Change: The AML IT systems in place do not trace appropriately the transactions below €1.000, since the name of the customer is not recorded. Moreover, in terms of transaction volume, the majority of AML IT systems lack sufficient parameterization for identifying complex and sophisticated scenarios (e.g. large amounts of low-denomination banknotes that are exchanged for higher-denominations and vice versa). In addition, deficiencies were identified in the operation of AML systems, related to the risk classification of clients, the completeness of their identification data and sanctions' screening.

Financial Leasing, Factoring and Credit Companies: Based on the information received, the companies have established appropriate AML IT systems for record keeping, monitoring, and STR reporting to support their AML policies and procedures, capitalizing on their strong ownership relationships with the Banking Sector. Nevertheless, no STRs have been reported in the last 3 years.

8. DESIGNATED NON-FINANCIAL BUSINESSES AND PROFESSIONS

8.1. Overview of Designated Non-Financial Businesses and Professions

Pursuant to the provisions of article 5(1) of Law 3691/2008, the obliged persons of the Designated Non-Financial Businesses and Professions (DNFBPs) are:

- Chartered auditors-accountants, audit firms, independent accountants and private auditors.
- Tax advisors and tax advisory firms (assessed in the report together with accountants).
- Real estate agents and related firms (realtors).
- Casino enterprises and casinos operating on ships flying the Greek flag, as well as public or private sector enterprises, organizations and other bodies that organize and/or conduct gambling and related agencies (assessed in the report as two activities: land-based and on-line gambling).
- Auction houses.
- Dealers in high-value goods²²⁹, only to the extent that payments are made in cash in an amount of fifteen thousand (15,000) Euros or more, whether the transaction is executed in a single operation or in several operations that appear to be linked.
- Auctioneers (assessed in the report together with auction houses).
- Pawnbrokers.
- Notaries and lawyers, when they participate, whether by acting on behalf of and for their clients in any financial or real estate transaction, or by assisting in the planning and execution of transactions for their clients, as defined in case m, article 5(1) of Law 3691/2008 (assessed in the report as two different activities).
- Natural or legal persons providing services to companies and trusts (Trusts and Company Service Providers), except tax advisors, notaries and lawyers, which by way of their business provide specific services to third parties (not assessed in the report, as no such natural or legal persons operate in Greece).

Pursuant to the provisions of article 6 of Law 3691/2008 as in force, the Competent Authorities supervising the above obliged persons are:

- The Hellenic Accounting and Auditing Standards Oversight Board (HAASOB) for chartered auditors-accountants.
- The Independent Authority for Public Revenue (Directorate General of Tax Administration) for:
 - accountants - tax advisors,
 - real estate agents,
 - auction houses,
 - Dealers in high-value goods,
 - Pawnbrokers.
- The Hellenic Gaming Commission (HGC) for gambling (land-based and on-line).

²²⁹ As defined in J.M.D. 1077797/20542/DE-E/08.06.2010 (B 918)

- The Ministry of Justice, Transparency and Human Rights for notaries and lawyers.

The following Table shows the number of obliged persons of the DNFBPs, on the basis of data available either to Competent Authorities or to their collective bodies, as well as an estimate of their gross revenue as a percentage of GDP in 2015.

	SECTOR	TOTAL SIZE	PARTICIPATION PERCENTAGE OF GROSS INCOME IN GDP (2015)
1	Lawyers	42.001	0,01%
2	ExternalAccountants / Tax Advisors	2.246 legal persons &18.000 natural persons	0,25%
3	Notaries	3.072	0,07%
4	Pawnbrokers	437	0,00%
5	Real Estate Agents	4.000	0,03%
6	Land BasedGambling	12	0,92%
7	OnlineGambling	24	0,07%
8	Auditors	46 legal persons & 1.210 natural persons	0,12%
9	AuctionHouses	15	0,00%
*Indicative data for the size of subsectors, based on an estimate of total gross revenue as a percentage of GDP			

Table52- DNFBPssectors

As shown in the above Table, the DNFBPs feature a large number of obliged persons. Some of them are not represented by collective bodies (pawnbrokers and auction houses), while for others, which are represented by collective bodies, their participation therein is optional (real estate agents, dealers in high-value goods) and in others their participation is mandatory (Bar Association and Association of Notaries).

It is also clear that the DNFBPs account for a small percentage of GDP.

Regarding dealers in high-value goods, it is noted that while the number of sector participants is considered high, their trading volume - exceeding Euro 15,000 in cash - is considered particularly small, given the restrictions on the use of cash laid down by the tax legislation²³⁰. Consequently, the number of these transactions is estimated as negligible, but cannot be precisely determined. For this reason, the

²³⁰Article 20 of Law 3842/2010, as amended by article 69(2) of Law 4446/2016 and Article 23 of Law 4172/2013

above table does not include the number or the gross revenues of dealers in high-value goods as a percentage of GDP.

8.2. DNFBPs vulnerability assessment

Using the World Bank’s tool, a vulnerability assessment was conducted for all DNFBPs sectors, assessing all the individual variables. The overall vulnerability score for each business/profession is shown in the Table below.

	SECTOR	FINAL VULNERABILITY SCORE	
1	Lawyers	0,86	HIGH
2	ExternalAccountants / TaxAdvisors	0,83	HIGH
3	Notaries	0,80	HIGH
4	Pawnbrokers	0,78	MEDIUM HIGH
5	Real Estate Agents	0,77	MEDIUM HIGH
6	Traders in High-Value Goods	0,72	MEDIUM HIGH
7	Land-BasedGambling	0,70	MEDIUM HIGH
8	OnlineGambling	0,56	MEDIUM
9	Auditors	0,54	MEDIUM
10	Auction Houses	0,50	MEDIUM

Table53- Vulnerability assessment of DNFBPs sectors

It is therefore noted that the overall vulnerability of obliged persons of the DNFBPs range from Medium to High.

The legislative framework on the entire DNFBPs, which defines the obligations and in general the issues related to money laundering for obliged persons, is considered satisfactory. Differences exist between businesses/professions as regards the issue of regulatory acts by the Competent Authorities. However, the non-issuance of certain Decisions mainly affects some of the other variables that define vulnerability, such as supervision or the imposition of administrative sanctions, and is taken into account in their assessment.

The main finding of the vulnerability assessment of obliged persons of the DNFBPs is that there are significant deviations in the level of supervision exercised by their Competent Authorities.

A further finding is that none of the obliged persons of the DNFBPs have been subject to the administrative sanctions provided for in case of non-compliance with the obligations imposed by Law 3691/2008. This weakness is directly related to shortcomings in exercising supervision in the

businesses/professions in which these are observed, as a condition for sanctioning is the conduct of audits.

A further reason for this is that Article 52 of Law 3691/2008 does not differentiate sanctions between the financial and non-financial sector; as a result, the sanctions are very strict and disproportionate to the size of most undertakings operating in the DNFBPs. This weakness is expected to be resolved by the incorporation of Directive (EU) 2015/849.

Weaknesses in both supervision and sanctioning affect the level of compliance of the obliged persons. Consequently, businesses/professions with limited supervision also present a lower level of compliance.

Compliance is also affected by the information and knowledge available to the obliged persons in charge of money laundering issues. Tellingly, pawnbrokers, dealers in high-value goods and auction houses have been rated particularly poorly, in terms of both their level of knowledge and of their level of compliance.

These weaknesses mean that, over the last five years, a negligible number of reports has been sent by the majority of obliged persons of the DNFBPs to the Anti-Money Laundering, Counter-Terrorist Financing and Source of Funds Investigation Authority. This quantitative criterion confirms the weaknesses already analyzed as regards supervision, knowledge and compliance.

Furthermore, a key feature of the DNFBPs is that it mainly consists of small businesses or freelancers lacking the necessary resources (financial, human and logistical infrastructure) or know-how required to comply with the obligations imposed by Law 3691/2008 (designation of compliance officer, internal controls, IT system for client profiling, etc.).

Moreover, the lack of resources impedes the obliged persons' access to databases and information on beneficial owners, politically exposed persons, as well as independent sources of information that facilitate the creation and updating of their customers' transactional profile. These weaknesses are particularly evident as compared to the Financial Sector.

In addition to the above, the overall vulnerability of each business/profession is also determined by inherent factors such as sector size, the use of cash in transactions and the anonymous use of the products offered by the obliged persons. The report will present those variables, per obliged person, that affect the entire sector.

At this point, it is noted that the main difficulty in the assessment was the lack of statistics. For this reason, it was considered necessary to collect information by preparing and sending an anonymous-response questionnaire to obliged persons; the data were then processed to draw conclusions. For some businesses/professions (dealers in high-value goods, auction houses and pawnbrokers), interviews were chosen as the most appropriate method of collecting information. Reports in the Press were also taken into account for the assessment of individual variables.

Finally, the three following variables were assessed at national level, taking into account, inter alia, and the particularities of the DNFBPs;

- Availability and access to beneficial ownership information
- Availability of reliable identification infrastructure
- Availability of independent information sources

More specifically, the table below presents the ratings of all general input variables for all obliged persons of the DNFBPs, followed by a detailed description for each.

	INPUT VARIABLES	LAYWERS	ExternalAccountants / TaxAdvisors	Notaries	Pawnbrokers	Real Estate Agents	Traders in High Value Goods	LandBased Gambling	Online Gambling	Auditors	Auction Houses
1	Comprehensiveness of AML Legal Framework	VERY HIGH	CLOSE TO EXCELLENT	VERY HIGH	CLOSE TO EXCELLENT	CLOSE TO EXCELLENT	CLOSE TO EXCELLENT	HIGH	CLOSE TO EXCELLENT	CLOSE TO EXCELLENT	CLOSE TO EXCELLENT
2	Effectiveness of Supervision/Oversight Activities	CLOSE TO NOTHING	VERY LOW	VERY LOW	MEDIUM	VERY LOW	VERY LOW	HIGH	HIGH	VERY HIGH	VERY LOW
3	Availability and Enforcement of Administrative Sanctions	LOW	LOW	LOW	MEDIUM LOW	LOW	LOW	MEDIUM LOW	MEDIUM LOW	MEDIUM LOW	LOW
4	Availability and Enforcement of Criminal Sanctions	MEDIUM	MEDIUM	MEDIUM	MEDIUM	MEDIUM	MEDIUM	N/A	N/A	MEDIUM	MEDIUM
5	Availability and Effectiveness of Entry Controls	VERY HIGH	MEDIUM HIGH	VERY HIGH	MEDIUM HIGH	VERY LOW	CLOSE TO NOTHING	CLOSE TO EXCELLENT	CLOSE TO EXCELLENT	CLOSE TO EXCELLENT	CLOSE TO NOTHING
6	Integrity of Business/Profession Staff	HIGH	MEDIUM HIGH	HIGH	CLOSE TO NOTHING	MEDIUM	MEDIUM	HIGH	HIGH	VERY HIGH	MEDIUM
7	AML Knowledge of Business/Profession Staff	MEDIUM HIGH	MEDIUM	MEDIUM HIGH	CLOSE TO NOTHING	LOW	CLOSE TO NOTHING	HIGH	HIGH	VERY HIGH	CLOSE TO NOTHING
8	Effectiveness of ComplianceFunction	CLOSE TO NOTHING	VERY LOW	VERY LOW	CLOSE TO NOTHING	CLOSE TO NOTHING	CLOSE TO NOTHING	HIGH	VERY HIGH	VERY HIGH	CLOSE TO NOTHING
9	Effectiveness of Suspicious Activity Monitoring and Reporting	CLOSE TO NOTHING	CLOSE TO NOTHING	LOW	CLOSE TO NOTHING	CLOSE TO NOTHING	CLOSE TO NOTHING	HIGH	MEDIUM HIGH	VERY HIGH	CLOSE TO NOTHING
10	Availability and Access to Beneficial Ownership Information	MEDIUM LOW	MEDIUM LOW	MEDIUM LOW	MEDIUM LOW	MEDIUM LOW	MEDIUM LOW	N/A	N/A	MEDIUM LOW	MEDIUM LOW
11	Availability of Reliable Identification Infrastructure	MEDIUM	MEDIUM	MEDIUM	MEDIUM	MEDIUM	MEDIUM	HIGH	HIGH	MEDIUM	MEDIUM
12	Availability of Independent Information Sources	MEDIUM HIGH	MEDIUM HIGH	MEDIUM HIGH	MEDIUM HIGH	MEDIUM HIGH	MEDIUM HIGH	MEDIUM HIGH	MEDIUM HIGH	MEDIUM HIGH	MEDIUM HIGH

Table54- DNFBPsectors: Assessment of input variables

8.3. Lawyers

8.3.1. General variables

8.3.1.1. Comprehensiveness of anti-money laundering (AML) legal framework

Assessment Rating: Very High (0.8)

The AML legal framework is highly reliable and near-comprehensive in accordance with Law 3691/2008²³¹. In addition, decision No. 59467/13.07.2009 of the Minister of Justice set out the details for the application of the individual obligations of lawyers and notaries (due diligence measures, keeping of records and data and disciplinary sanctions).

8.3.1.2. Effectiveness of supervision / oversight activities

Assessment Rating: Close to Nothing (0.1)

Pursuant to Law 3691/2008, the Competent Authority for the Supervision of Lawyers, regarding the implementation of the provisions of Law 3691/2008, is the Ministry of Justice, Transparency and Human Rights. In the framework of its supervision, the Ministry issued Ministerial Decision No. 59467/13.07.2009, as above.

Deficiencies in the supervision of lawyers include the non-recording of policies and procedures relating to supervision, the failure to issue manuals thereon, a lack of adequate staff trained in anti-money laundering issues, the non-availability of a monitoring mechanism and other supportive infrastructure for conducting on-site inspections in the context of supervising the obliged persons.

Given the above, no inspections on the implementation of due diligence measures for lawyers have been conducted during the last five years and there is no planning for such inspections based on risk analysis techniques.

In view of the above, it is noted that there are serious weaknesses in the supervision of lawyers and thus the variable was rated as Close to Nothing.

8.3.1.3. Availability and enforcement of administrative sanctions

Assessment Rating: Low (0.3)

Article 52 of Law 3691/2008 stipulates that, in the event of non-compliance with the obligations of the provisions of said law, the Competent Authorities may impose on obliged persons within their remit, cumulatively or disjunctively, either the taking of specific corrective measures within a certain period of time, or particularly strict sanctions. The same article provides for the referral of the obliged person to the instrument responsible for its disciplinary control.

Furthermore, decision No. 59467/13.07.2009 of the Minister of Justice stipulated the procedure for the referral of lawyers to the Bar Association in case of violation of the obligations set forth by Law 3691/2008.

However, a weakness is noted in the enforcement of administrative sanctions. The main reasons for the non-enforcement of the stipulated administrative sanctions are the failure of the Ministry of Justice,

²³¹Articles 12-26, 29, 31, 33, 35, 41, 43 of Law 3691/2008

Transparency and Human Rights to carry out the relevant inspections and the Competent Authority's failure to issue a relevant decision determining the degree of importance of each obligation and the criteria for determining sanctions, in case of non-compliance. The delay in issuing the decision is due to the fact that article 52(3) of Law 3691/2008 refers only to legal persons and not to natural persons. Moreover, the sanctions provided for are particularly severe; this acts as a deterrent to their enforcement, given that a large number of lawyers are freelancers and hence natural and not legal persons.

8.3.1.4. Availability and enforcement of criminal sanctions

Assessment Rating: Medium (0.5)

Article 45 of Law 3691/2008 provides for the enforcement of criminal sanctions on obliged persons in the event of a deliberate failure to report a suspicious transaction (STR) or of sending false data, while also defining the criminal sanctions in the event of the offense of money laundering. Criminal sanctions are also provided for all the predicate offenses referred to in Article 3 of Law 3691/2008, either under the Criminal Code (criminal organization, terrorist acts and terrorist financing, bribery, trafficking in human beings, computer fraud, etc.) or under other provisions (e.g. Article 66 of Law 4174/2013 on tax evasion). Criminal sanctions are enforced by the competent Courts. However, the statistics of the Court Services do not record the occupation of the person on whom the criminal sanctions have been imposed; thus, no data are available on the criminal sanctions imposed on each category of obliged person, and consequently on lawyers, either for money laundering or for any other predicate or ancillary offense. Indications of the involvement of lawyers in the above criminal offenses arise only from reports in the press.

8.3.1.5. Availability and effectiveness of entry controls

Assessment Rating: Very High (0.8)

As described in the Code on Lawyers (Law 4194/2013, A 208), a decision by the Ministry of Justice, Transparency and Human Rights on the appointment²³² of successful candidates, following examinations²³³, is required for those who wish to work as lawyers.

8.3.1.6. Integrity of business/profession staff

Assessment Rating: High (0.7)

Law firms employ both other lawyers as well as auxiliary staff that does not deal with handling cases. However, even if working in a law firm, lawyers do not fall into the category of "staff" because they maintain their scientific independence²³⁴ and are in themselves obliged persons under the provisions of Law 3691/2008.

In addition, the Code on Lawyers stipulates that inter-branch associations are prohibited²³⁵.

Therefore, this variable cannot be assessed as regards the staff and was assessed only as to the integrity of the profession of lawyer.

²³²Article 23 of the Code on Lawyers

²³³Articles 18-22 of the Code on Lawyers

²³⁴Article 48(1) of the Code on Lawyers

²³⁵Article 49(1) of the Code on Lawyers

8.3.1.7. AML Knowledge of business/profession staff

Assessment Rating: Medium High (0.6)

Although no training programs have been held to train lawyers on money laundering issues, either by their Competent Authority or by the country's Bar Associations, the nature of the particular function is such that it provides lawyers with access to legal databases and constant information on any changes to the legislative framework. For this reason, this variable was rated as Medium High.

8.3.1.8. Effectiveness of compliance function

Assessment Rating: Close to Nothing (0.1)

Pursuant to Article 41 of Law 3691/2008, obliged persons must apply adequate and appropriate policies and procedures in order to comply with the obligations laid down by said law. However, there is no evidence confirming that lawyers have in place and implement any compliance program.

The weaknesses identified in the effectiveness of compliance are partly due to the lawyers' incomplete information regarding their obligations, while it is also noted that lawyers are mostly freelancers, meaning that they have no designated compliance or internal audit officers.

Finally, it should be noted that the provisions of Law 3691/2008, as well as other regulatory acts, do not provide for the lawyers' obligation to designate a compliance officer or to carry out internal audits.

8.3.1.9. Effectiveness of suspicious activity monitoring and reporting

Assessment Rating: Close to Nothing (0.1)

Chapter F of Law 3691/2008 provides for the obligations of obliged persons in relation to record-keeping and the keeping of statistical data and information. In particular, this obligation is also imposed on lawyers by virtue of Decision No. 59467/15.07.2009 of the Minister of Justice.

Lawyers store their clients' data that are necessary in the context of their professional activity. However, it is not confirmed that all files and data set forth by Law 3691/2008 are stored (for client profiling), and their computerized storage²³⁶, which facilitates the detection of suspicious transactions, is not mandatory.

As regards the sending of suspicious transaction reports by lawyers, the establishment of a Lawyers' Committee is foreseen²³⁷, which receives their reports on suspicious or abnormal activities or transactions, checks whether they are submitted in accordance with the provisions of the above law and sends them to the FIU. Decision No. 67473/23.04.2009 of the Minister of Justice detailed the operation of the Lawyers' Committee and the procedure for submitting reports.

However, the Committee foreseen by the above provisions has not met yet, and therefore no reports have been sent to the FIU.

²³⁶ Article 37 of Law 3691/2008

²³⁷ Article 34 of Law 3691/2008

8.3.2. Inherent vulnerability (High)

The key factors affecting the inherent vulnerability of the Business/Profession are analyzed as follows:

8.3.2.1. Total size/volume of the business/profession

Assessment Rating: High

Both quantitative and qualitative criteria were used to assess the overall size of the Business/Profession. In particular, the quantitative criteria include gross revenue as a percentage of GDP in 2015 and the number of obliged persons.

More specifically, it is noted that, in Greece, 42,001 lawyers are registered as active in the registers of the country's Bar Associations. In their overwhelming majority, lawyers deal with everyday civil law issues. It is estimated that about 10% of lawyers provide services of considerable economic significance, relating to undertakings in Greece or abroad, which concern their establishment, operation and overall management, as well as collaborations amongst them.

Regarding the gross revenue of lawyers, it is noted that, according to a relevant study,²³⁸ legal services are included in the sectors with the highest tax evasion rates and therefore their gross revenue may be underestimated.

The qualitative criteria include lawyers' contribution to activities through which money laundering may be committed. In this context, it is noted that lawyers participate as advisors in negotiations concerning the establishment of legal entities, and provide services not only to legal entities seated in Greece but also to those seated in European Union countries or in third countries, including offshore companies and trusts. Furthermore, lawyers may also work as insolvency trustees²³⁹.

Regarding the participation of lawyers in property sales, it is noted that, as of 01.01.2014,²⁴⁰ a lawyer's attendance is optional for all contracting parties. However, many property buyers wish for a lawyer to inspect the deeds at the relevant land registry, and in most cases also wish them to attend the drafting of the contract.

In any case, the lawyers' legal knowledge and their easy access to various services and authorities attract those who seek to commit money laundering or tax evasion. Services relating to complex financial transactions, transactions with legal entities that are inactive, in liquidation or bankruptcy, the establishment or cooperation with offshore companies, trusts or phoenix companies are especially vulnerable.

For all the above reasons, the size of the business sector, as compared to the rest of DNFBPs, is considered High.

8.3.2.2. Client-base profile of the business/profession

Assessment Rating: Very High

Pursuant to Article 41 of Law 3691/2008, in the context of internal procedures, obliged persons must carry out a risk assessment in relation to their clients, in order to determine the extent²⁴¹ of the due

²³⁸ Artavanis Nikolaos et al. "Measuring Income Tax Evasion using Bank Credit: Evidence from Greece." Chicago Booth Research Paper, 25 Sept. 2015

²³⁹ Pursuant to P.D. 133/2016

²⁴⁰ Case 8a, subparagraph 1, par. M of the first article of Law 4093/2012 and Article 165(5) of Law 4194/2013

²⁴¹ Article 13(10) of Law 3691/2008

diligence measures they apply for each degree of risk, which depends on the type and financial size of the client, the business relationship, the product or the transaction.

In addition, increased due diligence measures are applied for Politically Exposed Persons. However, there is no Register of Politically Exposed Persons and only certain obliged persons have access to databases, against payment.

Lawyers' clients include natural and legal persons from the entire spectrum of the economy, including high-net-worth individuals, Politically Exposed Persons²⁴², but also legal entities with a complex or opaque structure. The frequency with which a lawyer may encounter high-risk clients can only be estimated, as no statistics are available. However, it is obvious that, in exercising their function, lawyers often have clients who have a criminal record or have been imposed other sanctions.

In view of the above, the profile of lawyers' clients is estimated to entail a very high risk.

8.3.2.3. Level of cash activity associated with the business/profession

Assessment Rating: High

Pursuant to tax law,²⁴³ transactions of over 500 Euros are paid exclusively through the use of cards or other electronic payment instruments. Payment for such items is not allowed in cash.

However, the Plenary of Presidents of Greek Bar Associations decided that, following Opinion 3/2017 of the Data Protection Authority, the installation and placement of POS devices (for card payments) is optional for lawyers.

It is also noted that lawyers' transactions often concern amounts of less than five hundred Euros, for which the use of electronic payment instruments is not mandatory. For this reason, the level of activities that are paid for in cash is considered High.

8.4. Accountants - Tax advisors

8.4.1. General variables

8.4.1.1. Comprehensiveness of anti-money laundering (AML) legal framework

Assessment Rating: Close to Excellent (0.9)

Based on the criteria of the variable, it was found that the AML legal framework is highly reliable and near-comprehensive in accordance with Law 3691/2008²⁴⁴.

In the context of informing the obliged persons in its remit - as the Competent Authority for Accountants and Tax advisors - the IAPR's Directorate General of Tax Administration has issued Decisions and circulars²⁴⁵ complementing and strengthening the legislative framework for combating money laundering and terrorist financing.

²⁴² Articles 19 and 22 of Law 3691/2008

²⁴³ Article 20 of Law 3842/2010, as amended by article 69(2) of Law 4446/2016 and Article 23 of Law 4172/2013

²⁴⁴ Articles 12-26, 29, 31, 33, 35, 41, 43 of Law 3691/2008

²⁴⁵ Circ. NO.1185/2013, Circ. No.1067/2011, Circ. No.1196/2012, Circ. DEL D 1191051 EX 2017/20.12.2017, Decision of the Minister of Finance 1051027/20340/DE-E/20.04.2010 (OG B 605), Circ. No.1127/2010

8.4.1.2. Effectiveness of supervision / oversight activities

Assessment Rating: Very Low (0.2)

In accordance with Law No. 3691/2008, the Competent Authority for supervising the implementation of the provisions of Law 3691/2008 by accountants - tax advisors is the IAPR's Directorate General of Tax Administration.

In the context of supervision, the Directorate General of Tax Administration periodically informs the obliged persons within its remit²⁴⁶, as well as the IAPR's auditors²⁴⁷ by issuing documents, guidelines and manuals, either in writing or by posting them on the IAPR's website.

Regarding the training of IAPR auditors and other officers, it is noted that in the 2012-2013 period, 14 seminars were held in the framework of Technical Assistance to Greece in the field of money laundering and combating tax evasion; the training programs held for the IAPR's auditors from September - December 2013 included, inter alia, information on money laundering and terrorist financing issues. IAPR officers also participated in an annual seminar of the OECD International Academy for Tax Crime Investigation.

Despite the above, there are serious weaknesses in the supervision of accountants - tax advisors. The most important are the failure to update the policies and procedures regarding the supervision of obliged persons in the remit of the IAPR's Directorate General of Tax Administration, the failure to issue recent manuals and instructions to auditors and the failure to carry out relevant inspections on accountants - tax advisors over the past five years.

In view of the above, it is noted that there are serious weaknesses in the supervision of accountants - tax advisors and thus the variable was rated as Very Low.

8.4.1.3. Availability and enforcement of administrative sanctions

Assessment Rating: Low (0.3)

Article 52 of Law 3691/2008 provides for the enforcement of corrective measures or administrative sanctions by the Competent Authorities to obliged persons in their remit, in the event of non-application of the due diligence measures and other obligations laid down in Law 3691/2008.

A major weakness concerns the enforcement of administrative sanctions, mainly involving the failure of the IAPR's Directorate General of Tax Administration to carry out the relevant audits. Another important reason is the non-issuance of a Decision by the Competent Authority, defining the degree of importance of each obligation, with an indication of the potential sanctions for non-compliance with such and other criteria for determining sanctions. The delay in issuing the Decision is due to the fact that the relevant authorizing provision²⁴⁸ refers only to legal persons and not to natural persons.

A disincentive for the enforcement of sanctions is that the sanctions provided for are particularly severe for accountants - tax advisors, given that many of them are freelancers, i.e. natural and not legal persons.

Finally, 55% of the accountants - tax advisors who responded to the anonymous questionnaire and, in particular, to the question of whether they are aware of the stipulated administrative sanctions,

²⁴⁶ Similarly to the previous footnote, as well as the FATF Public Statement and the results of its Plenary sessions (three times a year)

²⁴⁷ IAPR Decision DEL D 1117287 EX 2013/23.07.2013, OECD manuals in Greek (Decision DEL D 1012476 EX 2013/22.01.2013 and Decision DEL E 1050451 EX 2015/17.04.2015 of the Audits Directorate), FATF Public Statement and the results of its Plenary sessions (three times a year)

²⁴⁸ Article 52(3) of Law 3691/2008

responded positively, while 83% believe that they will be imposed administrative sanctions in case of non-compliance with the obligations arising from the provisions of Law 3691/2008 and other regulatory acts.

8.4.1.4. Availability and enforcement of criminal sanctions

Assessment Rating: Medium (0.5)

Article 45 of Law 3691/2008 provides for the enforcement of criminal sanctions on obliged persons in the event of a deliberate failure to report a suspicious transaction (STR) or of sending false data, while also defining the criminal sanctions in the event of the offense of money laundering. Criminal sanctions are also provided for all the predicate offenses referred to in Article 3 of Law 3691/2008, either under the Criminal Code (criminal organization, terrorist acts and terrorist financing, bribery, trafficking in human beings, computer fraud, etc.) or under other provisions (e.g. Article 66 of Law 4174/2013 on tax evasion).

Criminal sanctions are enforced by the competent Courts. However, the statistics of the Court Services do not record the occupation of the person on whom the criminal sanctions have been imposed; thus, no data are available on the criminal sanctions imposed on each category of obliged person, and consequently on accountants - tax advisors, either for money laundering or for any other predicate or ancillary offense. Indications of the involvement of accountants - tax advisors in the above criminal offenses arise only from reports in the press.

Finally, with regard to the knowledge of the criminal sanctions provided by the legislative framework, 51% of accountants - tax advisors replied that they knew them, while 81% believe that said criminal sanctions shall be imposed in case of non-compliance with the obligations set forth by the legislative framework.

8.4.1.5. Availability and effectiveness of entry controls

Assessment Rating: Medium High (0.6)

Article 1 of Law 2515/1997 (A 154) and P.D. 340/1998 regulate the issues concerning the profession of accountants - tax advisors and their professional identity.

In particular, in accordance with the provisions of P.D. 340/1998, as amended by sub-section H.5 of the first Article of Law 4093/2012, (A 222) and Article 20 of Law 4111/2013 (A 18), a professional identity card is issued to those wishing to work professionally as accountants - tax advisors, after they have submitted a relevant announcement, started pursuing their profession and following approval by the Central Administration or the Local Administrations of the Regional Departments of the Economic Chamber of Greece (ECG).

Furthermore, pursuant to the provisions of Law 4093/2012 (Section H), accountants - tax advisors are required to submit to the ECG, within the first two months of each year, a solemn declaration stating that they pursue the profession of accountant - tax advisor, that they have not been irrevocably convicted of the offenses referred to in Article 14 of P.D. 340/1998, that they have not committed any disciplinary offense under the Code of Ethics for Accountants - Tax Advisors and that they have attended all the necessary training corresponding to their professional classification level, provided by the ECG.

As of December 2010, the ECG has linked the Registry of Accountants - Tax Advisors to the Taxisnet IT system of the Ministry of Finance. If the accountant - tax adviser is not identified by the ECG, they are not provided access to the application for electronic submission of the tax returns of their clients. The accountants' - tax advisors' details are checked by both bodies, thus ensuring the protection of businesses and taxpayers from illegal activities.

However, a key weakness is that for services other than electronic submission, such as tax or fiscal advisory services, the identification of the accountant - tax adviser and the verification of their professional identity is not possible, meaning that a part of accountants - tax advisors is not identified.

8.4.1.6. Integrity of business/profession staff

Assessment Rating: Medium High (0.6)

As of 2014, the Code of Ethics for Accountants applies (Decision of the Deputy Minister of Development and Competitiveness No. 57088/DIOE-1033/18.12.2013, GG B 3314) to all accountants - tax advisors, who are obliged to observe the stipulated rules and principles.

In the questionnaire's question on the availability of a staff integrity control mechanism, both during recruitment and during employment, 52% of accountants - tax advisors stated that they had such a mechanism. Despite the fact that a large part of accountants - tax advisors does not have the above mechanism, 98% of accountants - tax advisors stated to be certain of the integrity of their staff. Furthermore, only 3% of accountants - tax advisors questioned stated that cases of non-observance of the obligations under Law 3691/2008 had been observed, due to omissions or negligence of their staff, and that these were at most two per year.

Finally, only 18% of accountants - tax advisors questioned stated that they have a staff protection mechanism in cases of suspicious transaction reporting to the FIU.

8.4.1.7. AML knowledge of business/profession staff

Assessment Rating: Medium (0.5)

Although the ECG provides all accountants - tax advisors registered in the relevant Registry with the necessary training in accounting and tax matters, no training seminars have been held on money laundering, nor has the Competent Authority for accountants - tax advisors held any training programs.

The weaknesses identified in training in this business are in line with the responses of the accountants - tax advisors to the questionnaire. In specific, 58% of accountants - tax advisors answered positively to the question of whether they are aware of the procedures and obligations for compliance and reporting provided by Law 3691/2008, despite the fact that only 18% of them have attended a training program to keep up-to-date on the legislation, policies and procedures in place to combat money laundering and terrorist financing.

Moreover, despite the obligation arising from Article 42 of Law 3691/2008, only 13% of accountants - tax advisors had attended a relevant information program, while 42% of them consider that their staff is aware of the procedures and obligations for compliance and reporting provided by Law 3691/2008.

Meanwhile, 76% of accountants - tax advisors stated that the training program and the relevant material in their business are inadequate.

The above clearly show that, despite the fact that accountants - tax advisors have stated, at a satisfactory percent, that both they and their staff have knowledge on money laundering issues, their training is insufficient and thus the variable is rated as Medium.

8.4.1.8. Effectiveness of compliance function

Assessment Rating: Very Low (0.2)

Despite the obligation to implement adequate and appropriate policies and procedures²⁴⁹, only 25% of accountants - tax advisors who responded to the questionnaire stated that they had a compliance program.

Meanwhile, only 20% of accountants - tax advisors stated in the relevant question that they have designated a compliance officer.

It should also be noted that the provisions of Law 3691/2008, as well as other regulatory acts, do not provide for the obligation of accountants - tax advisors to designate a compliance officer or to carry out internal audits.

Finally, it is noted that many accountants - tax advisors work as freelancers, meaning that they have no designated compliance or internal audit officers.

8.4.1.9. Effectiveness of suspicious A.activity monitoring and reporting

Assessment Rating: Close to Nothing (0.1)

Chapter F of Law 3691/2008 provides for the obligations of obliged persons in relation to record-keeping and the keeping of statistical data and information.

Accountants - tax advisors are not obliged to use an IT system to monitor transactions with their clients. In the relevant question, only 8% of accountants - tax advisors questioned responded that they had such a system.

Regarding the sending of suspicious transaction reports, it is noted that despite the instructions²⁵⁰ issued by the Directorate General of Tax Administration to obliged persons within its remit regarding the obligation to send reports to the FIU, 64% of accountants - tax advisors stated in a relevant question that they are aware of this obligation, while 58% believe that their staff are aware of the reporting obligation.

However, the significant weaknesses regarding this variable are also evident from the fact that only two reports have been sent by accountants - tax advisors to the FIU over the past five years.

Therefore, the variable is rated as Close to Nothing.

8.4.2. Inherent vulnerability (High)

The key factors affecting the inherent vulnerability of the Business/Profession are analyzed as follows:

8.4.2.1. Total size/volume of the business/profession

Assessment Rating: Medium High

Both quantitative and qualitative criteria were used to assess the overall size of the Business/Profession. In particular, the quantitative criteria include the number of obliged persons and their gross revenue as a percentage of GDP in 2015.

In Greece, there are 2,246 accounting - tax advisory services firms and 30,000 individual accountants - tax advisors, of which 18,000 are independent of any other natural or legal person.

²⁴⁹ Article 41 of Law 3691/2008

²⁵⁰ Circ. No. 1067/2011, Circ. No. 1196/2012 and Circ. No. DEL D 1191051 EX 2017/20.12.2017 of the Audits Directorate

Furthermore, regarding the gross revenue of accountants - tax advisors, it is noted that, according to a scientific article,²⁵¹ accounting and legal services are included in the sectors with the highest tax evasion rates and therefore their gross revenue may be underestimated.

The qualitative criteria include accountants' - tax advisors' contribution to activities through which money laundering may be committed. In this context, it is noted that the operations of accountants - tax advisors include, on the one hand, tax compliance services, such as the preparation and signing of financial statements and tax returns, and, on the other, services relating to the establishment, operation and cessation of businesses (e.g. as insolvency trustees pursuant to P.D. 133/2016). It is noted that Greek law does not provide for the establishment of trusts.

Accountants - tax advisors also provide financial and tax advice to natural and legal persons and may manage the assets of their clients, while they may also be appointed as administrators of legal persons.

Due to the involvement of accountants - tax advisors in a broad range of economic operations and to their large number, the size of the business sector, as compared to the rest of DNFBPs, is considered Medium High.

8.4.2.2. Client-base profile of the business/profession

Assessment Rating: Very High

The clients of accountants - tax advisors come from the entire spectrum of the economy, including high-risk clients such as politically exposed persons²⁵², high-net-worth individuals and legal entities with a complex or opaque structure, in which it is difficult to identify the beneficial owner. The frequency with which an obliged person may encounter high-risk clients can only be estimated, as no statistics are available on this.

In view of the above, the profile of accountants' - tax advisors' clients is estimated to entail a Very High Risk.

8.4.2.3. Level of cash activity associated with the business/profession

Assessment Rating: High

Despite restrictions on the use of cash imposed by tax legislation²⁵³, and the obligation to accept card payment instruments, which applies to a large number of professionals, including accountants - tax advisors²⁵⁴, 68% of accountants - tax advisors stated in the questionnaire that they use cash in their transactions with clients. For this reason, the level of activities is considered High.

²⁵¹Artavanis Nikolaos et al. "Measuring Income Tax Evasion using Bank Credit: Evidence from Greece." Chicago Booth Research Paper, 25 Sept. 2015

²⁵² Articles 19 and 22 of Law 3691/2008

²⁵³ Article 20 of Law 3842/2010, as amended by article 69(2) of Law 4446/2016 and Article 23 of Law 4172/2013

²⁵⁴ Article 65 of Law 4446/2016 and Joint Ministerial Decision 45231/2017 (B 1445) of the Ministers of Economy and Development and Finance

8.5. Notaries

8.5.1. General variables

8.5.1.1. Comprehensiveness of anti-money laundering (AML) legal framework

Assessment Rating: Very High (0.8)

Based on the criteria of the variable, it was found that the AML legal framework is highly reliable and near-comprehensive in accordance with Law 3691/2008²⁵⁵. In addition, decision No. 59467/13.07.2009 of the Minister of Justice set out the details for the application of the individual obligations of lawyers and notaries (due diligence measures, keeping of records and data and disciplinary sanctions).

8.5.1.2. Effectiveness of supervision / oversight activities

Assessment Rating: Very Low (0.2)

Pursuant to Law 3691/2008, the Competent Authority for the supervision of the implementation of the provisions of Law 3691/2008 by Notaries is the Ministry of Justice, Transparency and Human Rights. In the framework of its supervision, the Ministry of Justice issued Ministerial Decision No. 59467/13.07.2009, specifying the details of the implementation of the notaries' individual obligations. All Notaries' Associations of the country have been informed of this Decision.

Given that the Competent Authority does not have trained staff, a monitoring mechanism, know-how and support infrastructure to carry out on-site inspections, no inspections have been carried out on notaries.

The deficiency is to a certain extent compensated by the yearly inspections carried out by the competent Prosecutors, which in part include issues related to the obligations stipulated by Law 3691/2008.

In view of the above, it is noted that there are serious weaknesses in the supervision of notaries and thus the variable was rated as Very Low.

8.5.1.3. Availability and enforcement of administrative sanctions

Assessment Rating: Low (0.3)

Notaries are also subject to the provisions of Article 52 of Law 3691/2008. Decision No. 59467/13.07.2009 of the Minister of Justice stipulated the procedure for the referral of notaries to the competent Notaries' Association in case of violation of the obligations set forth by Law 3691/2008, for the conduct of a disciplinary control.

A major weakness concerns the enforcement of administrative sanctions; the main reason is the failure of Ministry of Justice, Transparency and Human Rights to carry out the relevant audits.

A disincentive for the enforcement of sanctions is that the sanctions provided for are particularly severe for notaries, given that many of them are freelancers, i.e. natural and not legal persons.

Despite the difficulties in enforcing administrative sanctions, in completing the questionnaire, 65% of the notaries who participated in the survey responded that they are aware of the administrative sanctions

²⁵⁵ Articles 12-26, 29, 31, 33, 35, 41, 43 of Law 3691/2008

foreseen by the relevant legislation and 88% believe that they would be imposed in case of non-compliance with the obligations stipulated in the relevant provisions.

8.5.1.4. Availability and enforcement of criminal sanctions

Assessment Rating: Medium (0.5)

With respect to this variable, the preceding analysis on the corresponding variable for lawyers also applies for notaries²⁵⁶.

Additionally, based on their responses to the questionnaire, 70% of notaries are aware of the sanctions provided by Law 3691/2008, while 92% replied positively to the question of whether they believe that they would be imposed criminal sanctions in case of non-compliance with the obligations stipulated by these provisions.

8.5.1.5. Availability and effectiveness of entry controls

Assessment Rating: Very High (0.8)

Greece is one of the EU Member States in which “Latin-style” notaries are instituted.

According to this institution, notaries, who are always legal experts, are chosen following strict procedures and in such a way as to be able to fulfill the duties of a public official.

Notaries are appointed by the state and are subject to its regulations. The responsible body for their appointment is the Ministry of Justice, Transparency and Human Rights, which is also responsible for the entire selection process, in accordance with the principles of the Code on Notaries (Law 2830/2000, GG A 96)²⁵⁷.

8.5.1.6. Integrity of business/profession staff

Assessment Rating: High (0.7)

The notarial profession is autonomous and therefore notaries cannot work in an employment relationship (as employees) with another notary or notarial firms.

However, Article 153 of the Code on Notaries stipulates that, in exercising their functions, two or more notaries of the same county court region may set up a civil law company, while stipulating that inter-branch associations are prohibited.

Therefore, this variable cannot be assessed as regards the staff and was assessed only as to the integrity of the notarial profession.

8.5.1.7. AML knowledge of business/profession staff

Assessment Rating: Medium High (0.6)

Although no training programs have been held to train notaries on money laundering issues, either by their Competent Authority or by the country’s Notaries’ Associations, the nature of the particular function is such that it provides notaries with access to legal databases and constant information on any changes to the legislative framework.

²⁵⁶ Variable 2.1.1.4

²⁵⁷ Articles 19-27 of the Code on Notaries

This is also confirmed by the notaries' responses in the survey. In specific, although only 6% of notaries responding to the questionnaire's question stated that they had attended a training program on the legislation, policies and procedures stipulated for combating money laundering and terrorist financing, 74% of notaries who responded to the survey responded that they are aware of the compliance and reporting obligations provided by Law 3691/2008.

For this reason, this variable was rated as "Medium High".

8.5.1.8. Effectiveness of compliance function

Assessment Rating: Very Low (0.2)

Despite the fact that Article 41 of Law 3691/2008 provides for the implementation of adequate and appropriate policies and procedures by obliged persons, only 9% of notaries responding to the questionnaire's question stated that they had a compliance program in place.

This weakness is due both to inadequate supervision and to the notaries' inadequate information regarding their obligations. Moreover, the provisions of Law 3691/2008, as well as other regulatory acts, do not provide for the notaries' obligation to designate a compliance officer or to carry out internal audits.

Finally, it is noted that notaries work as freelancers, meaning that they have no designated compliance or internal audit officers.

8.5.1.9. Effectiveness of suspicious activity monitoring and reporting

Assessment Rating: Low (0.3)

Chapter F of Law 3691/2008, in conjunction with Decision No. 59467/15.07.2009 of the Minister of Justice, provides that notaries should keep records and data in paper or electronic form.

Notaries keep records in accordance with the provisions of the Code on Notaries²⁵⁸. However, the record-keeping format and method are not designed to facilitate the detection of suspicious activities, through customer profiling and risk analysis.

As regards the reporting of suspicious transactions by notaries, it is noted that although 77% of notaries are aware of the obligation to report suspicious transactions and activities to the FIU (based on responses to the questionnaire), only 87 reports have been sent over the last five years.

8.5.2. Inherent vulnerability (High)

The key factors affecting the inherent vulnerability of the Business/Profession are analyzed as follows:

8.5.2.1. Total size/volume of the business/profession

Assessment Rating: Medium High

Both quantitative and qualitative criteria were used to assess the overall size of the Business/Profession. In particular, the quantitative criteria include the number of obliged persons and their gross revenue as a percentage of GDP in 2015

There is a set number of notaries in the country. In particular, 3,569 permanent posts are envisaged, while the number of currently active notaries is estimated at 3,072.

²⁵⁸ Article 12 of the Code on Notaries

Furthermore, regarding the gross revenue of notaries, it is noted that, according to a relevant study,²⁵⁹ legal services are included in the sectors with the highest tax evasion rates and therefore their gross revenue is underestimated.

Regarding the qualitative criteria, it is noted that the services offered by notaries, both for the purchase of real estate and for the establishment of companies, may attract those who seek to commit money laundering. Given that the involvement of real estate agents in the purchase and sale of real estate is optional, the obligation to observe due diligence measures in such cases falls exclusively on notaries.

For all the above reasons, the size of the business sector, as compared to the rest of DNFBPs, is rated as “Medium High”.

8.5.2.2. Client-base profile of the business/profession

Assessment Rating: Very High

A key high-risk activity in which notaries are involved is the purchase and sale of real estate.

Notaries’ clients include natural and legal persons from the entire spectrum of the economy, including high-net-worth individuals, Politically Exposed Persons, as well as clients with a criminal record or transacting with foreign countries. Furthermore, the clients of notaries may be legal entities with a complex or opaque structure, and offshore companies, in which it is difficult to identify the beneficial owner. The frequency with which a notary may encounter high-risk clients can only be estimated, as no statistics are available.

In view of the above, the profile of notaries’ clients is estimated to entail a “Very High” Risk.

8.5.2.3. Level of cash activity associated with the business/profession

Assessment Rating: High

The vulnerability of the notarial profession is increased by the fact that the use of cash in real estate transactions is not prohibited. The use of cash results in an increased risk of tax evasion and, by extension, of money laundering.

It is noted, however, that in the case of the purchase or sale of real estate or the lease of hotels or tourist accommodations of more than 250,000 Euros, for which a third-country national is granted a residence permit,²⁶⁰ the price is paid by a crossed bank check or by another bank transaction, the specific details of which must be solemnly declared by the contracting parties to the notary who draws up the contract and records them therein. The use of cash has decreased since 2015 due to the capital controls.

Notwithstanding the above, in the questionnaire, 88% of notaries stated that the transactions they are involved in make use of cash and therefore the amount of cash activities in the business sector is considered to be high

²⁵⁹Artavanis Nikolaos et al. “Measuring Income Tax Evasion using Bank Credit: Evidence from Greece.” Chicago Booth Research Paper, 25 Sept. 2015

²⁶⁰ Article 20 of Law 421 2014

8.6. Pawnbrokers

8.6.1. General variables

8.6.1.1. Comprehensiveness of anti-money laundering (AML) legal framework

Assessment Rating: Close to Excellent (0.9)

Based on the criteria of the variable, it was found that the AML legal framework is highly reliable and near-comprehensive in accordance with Law 3691/2008²⁶¹.

In the context of informing the obliged persons in its remit - as the Competent Authority for Pawnbrokers - the IAPR's Directorate General of Tax Administration has issued Decisions and circulars²⁶² complementing and strengthening the legislative framework for combating money laundering and terrorist financing.

8.6.1.2. Effectiveness of supervision / oversight activities

Assessment Rating: Medium (0.5)

In accordance with Law No. 3691/2008, the Competent Authority for supervising the implementation of the provisions of Law 3691/2008 by pawnbrokers is the IAPR's Directorate General of Tax Administration.

In the context of supervision, the Directorate General of Tax Administration periodically informs the obliged persons within its remit²⁶³, as well as the IAPR's auditors²⁶⁴ by issuing and sending documents, guidelines and manuals, or by posting them on the IAPR's website.

The weaknesses in the supervision of pawnbrokers mainly relate to the failure to update the policies and procedures regarding the supervision of obliged persons in the remit of the IAPR's Directorate General of Tax Administration, the failure to issue recent manuals and instructions to auditors and the failure to carry out relevant audits on pawnbrokers over the past five years.

It is noted, however, that, specifically for pawnbrokers, certain obligations under Law 3691/2008 are the same with the obligations imposed on this business sector by Police Order 5A/2011: Decision No. 1010/10/5/2011 (B 1948) of the Chief of the Hellenic Police Force, issued on the basis of the provisions of Law 3919/2011, specifying, inter alia, the records pawnbrokers should keep.

In particular, the keeping of a single register is foreseen, recording the data relating to the purchases, sales or pledges made. The keeping of this register in essence also satisfies the implementation of due diligence measures in relation to customer identification.

In the above context, the Police conduct controls at pawnshops and keeps statistics, according to which the number of controls and violations during the period 2013-2017 (up to March 2017) was as follows:

²⁶¹ Articles 12-26, 29, 31, 33, 35, 41, 43 of Law 3691/2008

²⁶² Circ. No.1185/2013, Circ. No.1067/2011, Circ. No.1196/2012, Circ. DEL D 1191051 EX 2017/20.12.2017, Decision of the Minister of Finance 1051027/20340/DE-E/20.04.2010 (GG B 605), Circ. No.1127/2010

²⁶³ Similarly to previous footnote, as well as the FATF Public Statement and the results of its Plenary sessions (three times a year)

²⁶⁴ IAPR Decision DEL D 1117287 EX 2013/23.07.2013, OECD manuals in Greek (Decision DEL D 1012476 EX 2013/22.01.2013 and Decision DEL E 1050451 EX 2015/17.04.2015 of the Audits Directorate), FATF Public Statement and the results of its Plenary sessions (three times a year)

YEAR	AUDITS	VIOLATIONS
2013	590	178
2014	852	112
2015	6.143	126
2016	7.173	125
2017	560	6

Table 55- DNFBPs sector: Audits and violations in pawnshops

In view of the above, it is concluded that the vulnerability of pawnbrokers in relation to supervision is mitigated by the controls carried out by the Police, which concern certain obligations of pawnbrokers that are similar to those provided by Law 3691/2008. For this reason, this variable was rated as “Medium Low”.

8.6.1.3. Availability and enforcement of administrative sanctions

Assessment Rating: Medium Low (0.4)

Article 52 of Law 3691/2008 stipulates that, in the event of non-compliance with the obligations of the provisions of said law, the Competent Authorities may decide to impose on obliged persons within their remit, cumulatively or disjunctively, either the taking of specific corrective measures within a set period of time, or particularly strict administrative sanctions.

A key weakness is noted in the enforcement of administrative sanctions. The main reason for the non-enforcement of the stipulated administrative sanctions is the failure of the IAPR’s Directorate General of Tax Administration to carry out the relevant inspections.

However, the records of the controls carried out by the Police at pawnshops show that it identified the following violations during the period 2013-2017 (up to March 2017) and imposed the stipulated sanctions.

VIOLATIONS	2013	2014	2015	2016	2017	TOTAL SUM
394 Criminal Code	4	1	6	7	1	19
Police Regulation 5 ^A	174	110	107	118	5	514
L.2472/97 Hellenic Data Protection Authority			2			2
L.3910/2011 Tax Legislation		1	2			3

L.D.515/70 art.4 as amended with art. 3 L.D. 1037/71 About time limits, art.31L. 3904/2010 Rationalizing the award of criminal justice.			9			9
TOTAL SUM	178	112	126	125	6	547

Table 56- DNFBPs sector: Violations of pawnbrokers for the years 2013-2017

In particular, the 514 violations of “Police Order 5A” mostly concern the failure to correctly keep the register in which pawnbrokers are required to record their transactions and enter customer identification documents.

Finally, pawnbrokers appear not to be aware of the administrative sanctions of Law 3691/2008, as evidenced by the phone interviews conducted.

In view of the above, the enforcement of administrative sanctions is rated as “Medium-Low”.

8.6.1.4. Availability and enforcement of criminal sanctions

Assessment Rating: Medium (0.5)

Article 45 of Law 3691/2008 provides for the enforcement of criminal sanctions on obliged persons in the event of a deliberate failure to report a suspicious transaction (STR) or of sending false data, while also defining the criminal sanctions in the event of the offense of money laundering. Criminal sanctions are also provided for all the predicate offenses referred to in Article 3 of Law 3691/2008, either under the Criminal Code (criminal organization, terrorist acts and terrorist financing, bribery, trafficking in human beings, computer fraud, etc.) or under other provisions (e.g. Article 66 of Law 4174/2013 on tax evasion).

Criminal sanctions are enforced by the competent Courts. However, the statistics of the Court Services do not record the occupation of the person on whom the criminal sanctions have been imposed; thus, no data are available on the criminal sanctions imposed on each category of obliged person, and consequently on pawnbrokers, either for money laundering or for any other predicate or ancillary offense. Indications of the involvement of pawnbrokers in the above criminal offenses arise only from reports in the press.

Finally, as evidenced by the phone interviews conducted, pawnbrokers appear not to be aware of the stipulated criminal sanctions.

8.6.1.5. Availability and effectiveness of entry controls

Assessment Rating: Medium High (0.6)

Due to the nature of the pawnbroker’s profession and the high risk entailed in pledging, buying and selling used jewelry, valuables and other movable property, they are under obligation to announce the commencement of their business to the relevant Security Department. The announcement is valid for five years; thereafter, a new announcement is required for the continuation of their professional activity, following the initial procedure.

Furthermore, Police Order 5A/2011 sets the conditions for pawnbrokers to exercise their profession; in order to ensure their integrity, these include the requirement that the person concerned must not have been convicted by final judgment of any sanction for a series of defined offenses.

In view of the above, this variable is rated as “Medium – High”.

8.6.1.6. Integrity of business/profession staff

Assessment Rating: Close to Nothing (0.1)

It is noted that although pawnbrokers state that they are confident about the integrity of their staff, reports in the Press link the pawnbroker’s profession to the committing of various offenses relating to money laundering, despite the current regulatory framework and the relevant controls. This fact highlights the integrity of the profession as a weakness; in fact, this is one of the reasons this profession was included in the list of obliged persons under Law 3691/2008.

8.6.1.7. AML knowledge of business/profession staff

Assessment Rating: Close to Nothing (0.1)

No training seminars on money laundering addressed to pawnbrokers have been organized by the Competent Authority for their supervision, i.e. the IAPR’s Directorate General of Tax Administration.

The weaknesses in training in this business sector are partly due to the absence of a collective instrument of pawnbrokers, which significantly impedes the Competent Authority’s communication with the specific obliged persons.

The staff of pawnshops has not attended any relevant information programs and do not appear to know the compliance and reporting procedures and obligations provided by Law 3691/2008.

Based on the above, it is concluded that pawnbrokers’ level of knowledge on money laundering issues is Close to Nothing.

8.6.1.8. Effectiveness of compliance function

Assessment Rating: Close to Nothing (0.1)

Pursuant to Article 41 of Law 3691/2008, obliged persons must apply adequate and appropriate policies and procedures as regards due diligence to the client and the other obligations laid down by said law.

Due to the serious weaknesses in their knowledge of money laundering issues and deficiencies in their supervision, pawnbrokers do not implement a compliance program, do not carry out internal audits on this issue and have no designated compliance officers.

8.6.1.9. Effectiveness of suspicious activity monitoring and reporting

Assessment Rating: Close to Nothing (0.1)

Chapter F of Law 3691/2008 provides for the obligations of obliged persons in relation to record-keeping and the keeping of statistical data and information.

Pawnbrokers are not obliged to use an IT system to monitor transactions with their clients. However, Police Order 5A/2011 provides for the keeping of a register of all transactions.

Regarding the sending of suspicious transaction reports, on the basis of the obligations laid down in Article 26 of Law 3691/2008, it is noted that, despite the instructions²⁶⁵ issued by the Directorate General of Tax Administration to obliged persons within its remit regarding the obligation to send reports to the FIU., pawnbrokers do not appear to be aware of this obligation. This is also evidenced by the fact that no reports have been sent to the FIU over the last five years.

8.6.2. Inherent vulnerability (Medium High)

The key factors affecting the inherent vulnerability of the Business/Profession are analyzed as follows:

8.6.2.1. Total size/volume of the business/profession

Assessment Rating: Medium Low

The financial crisis has led to a sharp increase in this profession in recent years. The submission of the relevant announcements began after the publication of Police Order 5A/2011; most of these, namely 649 announcements, were submitted in 2012. It is estimated that there are 437 active businesses in the sector, many of which have branches throughout the country.

The core business of pawnbrokers is the pledging, sale and purchase of used jewellery, valuables and other movable property. Considering all of the above, the size of the business sector, as compared to the rest of DNFBPs, is considered “Medium Low”.

8.6.2.2. Client-base profile of the business/profession

Assessment Rating: Very High

Pawnbrokers’ clients include natural persons from the entire spectrum of the economy, including clients with a criminal record or with interests in foreign countries. The frequency with which a pawnbroker may encounter high-risk clients can only be estimated, as no statistics are available.

In view of the above, the profile of pawnbrokers’ clients is estimated to entail a Very High Risk.

8.6.2.3. Level of cash activity associated with the business/profession

Assessment Rating: Very High

Despite the relevant tax legislation,²⁶⁶ which restricts the use of cash to transactions of under five hundred (500) Euros with natural persons, pledging is directly linked to the use of cash and thus the particular sector uses cash extensively in its transactions.

8.6.2.4. Other vulnerable factors of the business/profession: Use of the business/profession in fraud or tax evasion schemes

Assessment Rating: Exists and is Significant

According to several reports in the Press and investigations, the profession of pawnbroker is linked to various financial and other offenses. Although there are no relevant statistics, the involvement of this business sector in tax evasion or other types of fraud is considered to exist, to a significant degree.

²⁶⁵Circ. No. 1067/2011, Circ. No. 1196/2012 and Circ. No. DEL D 1191051 EX 2017/20.12.2017 of the Audits Directorate

²⁶⁶Article 20 of Law 3842/2010, as amended by article 69(2) of Law 4446/2016 and Article 23 of Law 4172/2013,

8.7. Real estate agents

8.7.1. General variables

8.7.1.1. Comprehensiveness of anti-money laundering (AML) legal framework

Assessment Rating: Close to Excellent (0.9)

Based on the criteria of the variable, it was found that the AML legal framework is highly reliable and near-comprehensive in accordance with Law 3691/2008²⁶⁷.

In the context of informing the obliged persons in its remit - as the Competent Authority for real estate agents - the IAPR's Directorate General of Tax Administration has issued decisions and circulars²⁶⁸ complementing and strengthening the legislative framework for combating money laundering and terrorist financing.

8.7.1.2. Effectiveness of supervision / oversight activities

Assessment Rating: Very Low (0.2)

Pursuant to Law 3691/2008, the Competent Authority for supervising the application of the provisions of Law 3691/2008 by real estate agents is the IAPR's Directorate General of Tax Administration.

In the context of supervision, the Directorate General of Tax Administration periodically informs the obliged persons within its remit²⁶⁹, as well as the IAPR's auditors²⁷⁰ by issuing documents, guidelines and manuals, either in writing or by posting them on the IAPR's website.

Despite the above, there are serious weaknesses in the supervision of real estate agents. The most important are the failure to update the policies and procedures regarding the supervision, the failure to issue recent manuals and instructions to auditors and the failure to carry out relevant inspections on real estate agents over the past five years (with the exception of an inspection in 2012, in which failure to send an STR to the FIU was found).

In view of the above, it is noted that there are serious weaknesses in the supervision of real estate agents and thus the variable was rated as Very Low.

8.7.1.3. Availability and enforcement of administrative sanctions

Assessment Rating: Low (0.3)

Pursuant to article 52 of Law 3691/2008, the Competent Authorities may impose administrative sanctions on obliged persons in the event of non-compliance with the obligations set forth by Law 3691/2008.

A key weakness is noted in the enforcement of administrative sanctions. The key reasons for the non-enforcement of the stipulated administrative sanctions are the failure of the IAPR's Directorate General of Tax Administration to carry out the relevant inspections and the non-issuance of a relevant decision, defining the degree of importance of each obligation, with an indication of the potential sanctions for non-compliance with such and other criteria for determining sanctions.

²⁶⁷ Articles 12-26, 29, 31, 33, 35, 41, 43 of Law 3691/2008

²⁶⁸ Circ. No.1185/2013, Circ. No.1067/2011, Circ. No.1196/2012, Circ. DEL D 1191051 EX 2017/20.12.2017, Decision of the Minister of Finance 1051027/20340/ DE-E/20.04.2010 (GG B 605), Circ.. No.1127/2010

²⁶⁹ Similarly to the previous footnote, as well as the FATF Public Statement and the results of its Plenary sessions (three times a year)

²⁷⁰ IAPR Decision DEL D 1117287 EX 2013/23.07.2013, OECD manuals in Greek (Decision DEL D 1012476 EX 2013/22.01.2013 and Decision DEL E 1050451 EX 2015/17.04.2015 of the Audits Directorate), FATF Public Statement and the results of its Plenary sessions (three times a year)

Another disincentive for the enforcement of sanctions is that the sanctions provided for are particularly severe for real estate agents, given that many of them are freelancers, i.e. natural and not legal persons.

40% of the real estate agents who responded to the anonymous questionnaire and, in particular, to the question of whether they are aware of the stipulated administrative sanctions, responded positively, while 90% believe that they will be imposed administrative sanctions in case of non-compliance with the obligations arising from the provisions of Law 3691/2008 and other regulatory acts.

8.7.1.4. Availability and enforcement of criminal sanctions

Assessment Rating: Medium (0.5)

Article 45 of Law 3691/2008 provides for the enforcement of criminal sanctions on obliged persons in the event of a deliberate failure to report a suspicious transaction (STR) or of sending false data, while also defining the criminal sanctions in the event of the offense of money laundering. Criminal sanctions are also provided for all the predicate offenses referred to in Article 3 of Law 3691/2008, either under the Criminal Code (criminal organization, terrorist acts and terrorist financing, bribery, trafficking in human beings, computer fraud, etc.) or under other provisions (e.g. Article 66 of Law 4174/2013 on tax evasion).

Criminal sanctions are enforced by the competent Courts. However, the statistics of the Court Services do not record the occupation of the person on whom the criminal sanctions have been imposed; thus, no data are available on the criminal sanctions imposed on each category of obliged person, and consequently on real estate agents, either for money laundering or for any other predicate or ancillary offense. Indications of the involvement of real estate agents in the above criminal offenses arise only from reports in the press.

Finally, to the question of whether they are aware of the criminal sanctions provided by the legal framework, 40% of real estate agents responded that they were. In addition, 90% of real estate agents believe that they would be imposed these criminal sanctions if they do not comply with the obligations of the legislative framework.

8.7.1.5. Availability and effectiveness of entry controls

Assessment Rating: Very Low (0.2)

Pursuant to Article 198(4) of the Fourth Part of Law 4072/2012, pursuing the profession of real estate agent requires the registration of the interested person in the register of the competent Professional Chamber and in the General Commercial Register (GCR). The above article of this law stipulates the conditions for exercising the profession of real estate agent, including the non-conviction of the interested person for certain offenses set forth in these provisions. Meanwhile, Article 202 of the Fourth Part of Law 4072/2012 provides for criminal sanctions for those who conduct brokering operations or present themselves as real estate agents without fulfilling the conditions and without being registered in the GCR.

The conditions for pursuing the profession of real estate agent are minimal. No examination-based certification is required and there is no mandatory internship period. It is also not mandatory to attend training programs by already licensed real estate agents. It should be noted, however, that the Real Estate Federation of Greece (OMASE), in cooperation with the Hellenic Confederation of Professionals, Craftsmen and Merchants (GSVEE), will hold the first certification training on issues relating to the profession in 2018.

Finally, there is evidence that there are natural persons operating in this business sector without having been registered with the Professional Chamber. According to OMASE data, the number of illegal or non-professional real estate agents is actually greater than that of legitimate real estate agents. Specifically, while currently some 4,000 legitimate professionals work as real estate agents nationwide, it is estimated that at least 5,000 more people present themselves on the market as real estate agents and negotiate real estate purchases, sales and leases. Finally, it is noted that, in Greece, it is not mandatory for the transfer or lease of real estate to be mediated by a real estate agent.

8.7.1.6. Integrity of business/profession staff

Assessment Rating: Medium (0.5)

Regarding real estate brokers, it is noted that following the adoption of Law 4072/2012, which regulates issues pertaining to this profession, the OMASE proceeded with the issuance of a Code of Conduct, which details the specific obligations of real estate agents and introduces additional commitments towards their principals, colleagues and consumers, in order to strengthen the regulatory framework. This Code has not yet been approved by all local Associations.

Furthermore, in the questionnaire's question on the availability of a staff integrity control mechanism, both during recruitment and during employment, 29% of real estate agents stated that they had such a mechanism. Despite the fact that a large part of real estate agents does not have the above mechanism, 86% of real estate agents stated to be certain of the integrity of their staff.

Finally, only 17% of real estate agents questioned stated that they have a staff protection mechanism in cases of suspicious transaction reporting to the FIU.

8.7.1.7. AML knowledge of business/profession staff

Assessment Rating: Low (0.3)

No training seminars on money laundering addressed to real estate agents have been organized by their collective instruments of the Competent Authority for their supervision, i.e. the IAPR's Directorate General of Tax Administration.

The IAPR's Directorate General of Tax Administration has issued instructions to real estate agents, as detailed in the variable concerning supervision, but these require updating.

The weaknesses identified in training in this business are in line with the responses of the real estate agents to the questionnaire. In specific, 50% of real estate agents answered positively to the question of whether they are aware of the procedures and obligations for compliance and reporting provided by Law 3691/2008, despite the fact that only 20% of them have attended a training program to keep up-to-date on the legislation, policies and procedures in place to combat money laundering and terrorist financing.

Despite the provisions of article 42 of Law 3691/2008, which stipulates that obliged persons should take the necessary measures for their employees to become aware of the provisions of Law 3691/2008 and of the relevant regulatory decisions, only 14% of the staff of real estate agents have attended a relevant information program, while 43% of real estate agents stated that their staff are aware of the procedures and obligations for compliance and reporting set forth by Law 3691/2008.

Meanwhile, 83% of real estate agents stated that the training program and the relevant material in their business are inadequate.

The above clearly show that the training of both real estate agents and their employees is inadequate and therefore the variable is rated as Low.

8.7.1.8. Effectiveness of compliance function

Assessment Rating: Close to Nothing (0.1)

Pursuant to Article 41 of Law 3691/2008, obliged persons must apply adequate and appropriate policies and procedures as regards due diligence to the client and the beneficial owner, and the implementation of their other obligations laid down by said law.

However, only 30% of real estate agents who responded to the questionnaire stated that they had a compliance program in place.

The provisions of Law 3691/2008, as well as other regulatory acts, do not provide for real estate agents' obligation to designate a compliance officer or to carry out internal audits. This is due to the fact that many real estate agents work as freelancers, meaning that they have no designated compliance or internal audit officers.

8.7.1.9. Effectiveness of suspicious activity monitoring and reporting

Assessment Rating: Close to Nothing (0.1)

Chapter F of Law 3691/2008 provides for the obligations of obliged persons in relation to record-keeping and the keeping of statistical data and information.

Real estate agents are not obliged to use an IT system to monitor transactions with their clients. In the relevant question, the real estate agents questioned responded that they do not have such a system.

Regarding the sending of suspicious transaction reports, it is noted that despite the provisions of article 26 of Law 3691/2008 and the instructions²⁷¹ issued by the Directorate General of Tax Administration to obliged persons within its remit regarding the obligation to send reports to the FIU, 60% of real estate agents stated in a relevant question that they are aware of this obligation, while 43% believe that their staff are aware of this obligation.

However, the significant weaknesses regarding this variable are also evident from the fact that no STRs have been sent by real estate agents to the FIU over the past five years.

Therefore, the variable is rated as Close to Nothing.

8.7.2. Inherent vulnerability (Medium High)

The key factors affecting the inherent vulnerability of the Business/Profession are analyzed as follows:

8.7.2.1. Total size/volume of the business/profession

Assessment Rating: Medium Low

While currently some 4,000 legitimate professionals work as real estate agents nationwide, according to OMASE data, the number of practitioners in this profession is likely to be twice as high.

The services provided by real estate agents include recommendations or mediation for concluding contracts relating to real estate, and in particular contracts for the sale, exchange, rental, leasing, establishing of easements or for real estate exchange systems.

²⁷¹Circ. No. 1067/2011, Circ. No. 1196/2012 and circ. No. DEL D 1191051 EX 2017/20.12.2017 of the Audits Directorate

Real estate purchases and sales are internationally recognized as high-risk transactions, as many persons seeking to commit money laundering choose to do so through the purchase of real estate, as highlighted by the typologies published on this issue. Tax evasion has also been detected in many real estate transactions, thus indicating that real estate agents may be involved as facilitators in the above crimes.

However, in Greece, it is not mandatory for the conclusion of these contracts to be mediated by a real estate agent. This results in only part of the purchases of sales of real estate or other real estate contracts being concluded with the participation of a real estate agent.

Considering all of the above, the size of the business sector, as compared to the rest of DNFBPs, is considered Medium Low.

8.7.2.2. Client-base profile of the business/profession

Assessment Rating: Very High

A key high-risk activity in which real estate agents are involved is the purchase and sale of real estate. It is noted at this point that according to reports (Fortune survey 04.09.2015), foreign buyers of real estate in Greece come mainly from Europe (Germany, France, Italy), Arab countries (United Arab Emirates, Saudi Arabia, Egypt and Jordan) and China.

The clients of real estate agents include natural and legal persons from the entire spectrum of the economy, including high-net-worth individuals, Politically Exposed Persons²⁷², as well as clients with a criminal record or transacting with foreign countries. Furthermore, the clients of real estate agents may be legal entities with a complex or opaque structure, and offshore companies, in which it is difficult to identify the beneficial owner. The frequency with which a real estate agent may encounter high-risk clients can only be estimated, as no statistics are available.

In view of the above, the profile of real estate agents' clients is estimated to entail a Very High Risk.

8.7.2.3. Level of cash activity associated with the business/profession

Assessment Rating: High

The vulnerability of the profession of real estate agents is increased by the fact that the use of cash in real estate transactions is not prohibited. The use of cash results in an increased risk of tax evasion and, by extension, of money laundering.

It is noted, however, that in the case of the purchase or sale of real estate or the lease of hotels or tourist accommodations of more than 250,000 Euros, for which a third-country national is granted a residence permit²⁷³, the price is paid by a crossed bank check or by another bank transaction. Furthermore, aiming at restricting the use of cash, "Real estate agencies" were recently added to the categories of professionals²⁷⁴ who are obliged to accept electronic payment instruments.

Despite the above, given that real estate transactions are still being made using cash, the amount of such transactions is considered High.

²⁷² Articles 19 and 22 of Law 3691/2008

²⁷³ Article 20 of Law 4251/2014

²⁷⁴ Article 65 of Law 4446/2016 and Joint Ministerial Decision 133473/05.12.2017 (B 4309)

8.8. Dealers in high-value goods

8.8.1. General variables

8.8.1.1. Comprehensiveness of anti-money laundering (AML) legal framework

Assessment Rating: Close to Excellent (0.9)

Based on the criteria of the variable, it was found that the AML legal framework is highly reliable and near-comprehensive in accordance with Law 3691/2008²⁷⁵.

In the context of informing the obliged persons in its remit - as the Competent Authority for dealers in high-value goods - the IAPR's Directorate General of Tax Administration has issued Decisions and circulars²⁷⁶ complementing and strengthening the legislative framework for combating money laundering and terrorist financing.

8.8.1.2. Effectiveness of supervision / oversight activities

Assessment Rating: Very Low (0.2)

Pursuant to Law 3691/2008, the Competent Authority for supervising the application of the provisions of Law 3691/2008 by dealers in high-value goods is the IAPR's Directorate General for Tax Administration.

In the context of supervision, the Directorate General of Tax Administration periodically informs the obliged persons within its remit²⁷⁷, as well as the IAPR's auditors²⁷⁸ by issuing documents, guidelines and manuals, either in writing or by posting them on the IAPR's website.

Furthermore, regarding the training of IAPR auditors and other officers, in the period from June 2012 to December 2013, 14 seminars were held in the framework of Technical Assistance to Greece in the field of money laundering and combating tax evasion. In addition, the training programs held for the IAPR's auditors from September - December 2013 included, inter alia, information on money laundering and terrorist financing issues.

Despite the above, there are serious weaknesses in the supervision of dealers in high-value goods. The most important are the failure to update the policies and procedures regarding the supervision, the failure to issue recent manuals and instructions to auditors and the failure to carry out relevant inspections on dealers in high-value goods over the past five years (with the exception of three inspections in jewelry stores in 2012, in which no transactions of over 15,000 in cash were identified).

In view of the above, the supervision of dealers in high-value goods was rated as Very Low.

8.8.1.3. Availability and enforcement of administrative sanctions

Assessment Rating: Low (0.3)

Pursuant to article 52 of Law 3691/2008, the Competent Authorities may impose corrective measures and/or administrative sanctions on obliged persons in the event of non-compliance with the obligations set forth by Law 3691/2008.

²⁷⁵ Articles 12-26, 29, 31, 33, 35, 41, 43 of Law 3691/2008

²⁷⁶Circ. No.1185/2013, Circ. No.1067/2011, Circ. No.1196/2012, Circ.DEL D 1191051 EX 2017/20.12.2017, Decision of the Minister of Finance 1051027/20340/ DE-E/20.04.2010 (GG B 605), Circ. No.1127/2010

²⁷⁷ Similarly to the previous footnote, as well as the FATF Public Statement and the results of its Plenary sessions (three times a year)

²⁷⁸IAPR Decision DEL D 1117287 EX 2013/23.07.2013, OECD manuals in Greek (Decision DEL D 1012476 EX 2013/22.01.2013 and Decision DEL E 1050451 EX 2015/17.04.2015 of the Audits Directorate), FATF Public Statement and the results of its Plenary sessions (three times a year)

A key weakness is noted in the enforcement of administrative sanctions. The main reason for the non-enforcement of the stipulated administrative sanctions is the failure of the IAPR's Directorate General of Tax Administration to carry out the relevant inspections. Another important reason is the non-issuance of a relevant Decision, defining the degree of importance of each obligation, with an indication of the potential sanctions for non-compliance with such and other criteria for determining sanctions.

Finally, it is noted that dealers in high-value goods do not appear to know the administrative sanctions provided for by the above law.

8.8.1.4. Availability and enforcement of criminal sanctions

Assessment Rating: Medium (0.5)

Article 45 of Law 3691/2008 provides for the enforcement of criminal sanctions on obliged persons in the event of a deliberate failure to report a suspicious transaction (STR) or of sending false data, while also defining the criminal sanctions in the event of the offense of money laundering. Criminal sanctions are also provided for all the predicate offenses referred to in Article 3 of Law 3691/2008, either under the Criminal Code (criminal organization, terrorist acts and terrorist financing, bribery, trafficking in human beings, computer fraud, etc.) or under other provisions (e.g. Article 66 of Law 4174/2013 on tax evasion).

Criminal sanctions are enforced by the competent Courts. However, the statistics of the Court Services do not record the occupation of the person on whom the criminal sanctions have been imposed; thus, no data are available on the criminal sanctions imposed on each category of obliged person, and consequently on dealers in high-value goods, either for money laundering or for any other predicate or ancillary offense. Indications of the involvement of dealers in high-value goods in the above criminal offenses arise only from reports in the press.

Finally, it is noted that dealers in high-value goods do not appear to know the administrative sanctions provided for in the relevant legal framework.

8.8.1.5. Availability and effectiveness of entry controls

Assessment Rating: Close to Nothing (0.1)

Except for the registration of the interested person in the register of the competent Chamber of Commerce and in the General Commercial Register (GCR), there are no other specified conditions for exercising the profession of dealer.

8.8.1.6. Integrity of business/profession staff

Assessment Rating: Medium (0.5)

Despite not having a mechanism to control the integrity of their staff, both during recruitment and during employment at the company, dealers in high-value goods state that they are confident about their integrity.

Furthermore, dealers in high-value goods do not have a staff protection mechanism in cases of suspicious transaction reporting to the FIU.

8.8.1.7. AML knowledge of business/profession staff

Assessment Rating: Close to Nothing (0.1)

No training seminars on money laundering addressed to dealers in high-value goods or their staff have been organized by their collective instruments or by the Competent Authority for their supervision.

The IAPR's Directorate General of Tax Administration has issued instructions to dealers in high-value goods, as detailed in the variable concerning supervision, but these require updating.

The weaknesses in training in this business sector are in line with the low level of knowledge they stated as having as regards the procedures and obligations for compliance and reporting provided by the provisions of Law 3691/2008.

It is noted that dealers in high-value goods stress that the use of electronic payment instruments for transactions of over 15,000 Euros exempts them from any other obligation set forth in Law 3691/2008, as they are only considered obliged persons when conducting such transactions in cash.

8.8.1.8. Effectiveness of compliance function

Assessment Rating: Close to Nothing (0.1)

Pursuant to Article 41 of Law 3691/2008, obliged persons must apply adequate and appropriate policies and procedures as regards due diligence to the client and the beneficial owner, and the other obligations laid down by said law.

Notwithstanding the above obligation, dealers in high-value goods do not have a compliance program in place, as they do not consider themselves obliged persons, because they do not use cash in transactions of over 15,000 Euros.

The provisions of Law 3691/2008, as well as other regulatory acts, do not provide for the obligation of dealers in high-value goods to designate a compliance officer or to carry out internal audits. In this context, dealers have not proceeded to the corresponding actions for designating a compliance officer or carrying out internal audits.

8.8.1.9. Effectiveness of suspicious activity monitoring and reporting

Assessment Rating: Close to Nothing (0.1)

Chapter F of Law 3691/2008 provides for the obligations of obliged persons in relation to record-keeping and the keeping of statistical data and information.

However, pursuant to the provisions of article 37 of Law 3691/2008, dealers in high-value goods are not obliged to use an IT system to monitor transactions with their clients.

Regarding the obligation to send suspicious transaction reports pursuant to article 26 of Law 3691/2008, it is noted that despite the instructions²⁷⁹ issued by the Directorate General of Tax Administration to obliged persons within its remit regarding the obligation to send reports to the FIU, when asked, dealers in high-value goods stated that neither they nor their staff are aware of this obligation, while reiterating that they are not obliged persons, as they do not use cash in transactions of over 15,000 Euros.

The significant weaknesses regarding this variable are also evident from the fact that no STRs have been sent by dealers in high-value goods to the FIU over the past five years.

Therefore, the variable is rated as Close to Nothing.

8.8.2. Inherent vulnerability (Medium High)

The key factors affecting the inherent vulnerability of the Business/Profession are analyzed as follows:

²⁷⁹Circ. No. 1067/2011, Circ. No. 1196/2012 and Circ. No. DEL D 1191051 EX 2017/20.12.2017 of the Audits Directorate

8.8.2.1. Total size/volume of the business/profession

Assessment Rating: Medium

The business sector's size, as compared to the rest of DNFBPs, is considered Medium, because, while the number of companies operating in it is very large, the number of transactions of over 15,000 Euros made in cash is considered very small, due to the restrictions imposed by tax legislation²⁸⁰, which effectively allow transactions of over 500 Euros only through the use of electronic payment instruments.

8.8.2.2. Client-base profile of the business/profession

Assessment Rating: High

The clients of dealers in high-value goods include natural persons from the entire spectrum of the economy, including high-net-worth individuals, Politically Exposed Persons, as well as clients with a criminal record or transacting with foreign countries. The frequency with which a dealer in high-value goods may encounter high-risk clients can only be estimated, as no statistics are available. As expected, dealers with businesses in areas with tourist traffic have more foreign customers, but this does not mean that the risk increases, because they rarely come from high-risk countries.

However, none of the above categories of customers can be excluded and thus the profile of customers of dealers in high-value goods is estimated to entail a "High Risk".

8.8.2.3. Level of cash activity associated with the business/profession

Assessment Rating: Medium

According to the information they provided in their interviews, the use of cash by dealers is restricted to the amount of five hundred (500) Euros, as stipulated by tax legislation.

Meanwhile, aiming to further restrict the use of cash, an obligation was set on accepting card payment instruments for a large number of professionals, including dealers²⁸¹; a tax deduction is also granted if the taxpayer pays for acquiring goods and receiving services by electronic payment instruments²⁸². The restriction on the use of cash also achieves a reduction in anonymous transactions and improves tax compliance.

However, although the number of cash transactions worth over 500 Euros is estimated to be very small, cash transactions for acquiring goods worth less than 500 Euros are still widespread.

8.8.2.4. Other vulnerable factors of the business/profession: Non-face-to-face transactions with the client

Assessment Rating: Available and Prominent

Dealers often make transactions via the internet, as some also operate online stores in addition to bricks and mortar stores. However, transactions through online stores are made by electronic payment instruments.

²⁸⁰ Article 20 of Law 3842/2010, as amended by article 69(2) of Law 4446/2016 and Article 23 of Law 4172/2013

²⁸¹ Article 65 of Law 4446/2016

²⁸² Article 68 of Law 4446/2016

8.9. Land-based gambling

8.9.1. General variables

8.9.1.1. Comprehensiveness of anti-money laundering (AML) legal framework

Assessment Rating: High (0.7)

The Regulation specifies the implementation of the provisions of Law 3691/2008 in the gambling sector and determines: 1) the obliged persons²⁸³, 2) their obligations with regard to a) taking organizational measures (drawing up relevant policies, designation of a Compliance officer, staff education and training, monitoring of compliance); b) the implementation of due diligence measures; c) reporting to the FIU d) record keeping and 3) the procedure for carrying out compliance checks and taking corrective actions.

It is noted that casino enterprises (land based) and casinos operating on ships are regulated as to the implementation of measures on combating money laundering by the provisions of Law 3691/2008. The issuance of a regulatory decision specifying the implementation of the above measures by Casino enterprises is currently being finalized, while there is still no timetable for the implementation of a relevant regulatory framework for casinos operating on ships.

8.9.1.2. Effectiveness of supervision / oversight activities

Assessment Rating: High (0.7)

The oversight and supervision of the activities of the above obliged persons by the HGC as regards for ML/TF is exercised adequately, satisfactorily and impartially, as the HGC:

- Has full authority, under the law, to supervise the compliance of obliged persons in issues pertaining to money laundering.
- Performs such supervision, based on the regulatory framework it issues.
- Has the necessary expertise to assess the risk involved.
- Has a sufficient number of staff, trained and supplied with the necessary skills and knowledge, to conduct audits on issues pertaining to money laundering.
- Effects administrative supervision of the compliance of obliged persons with all obligations arising from the regulatory framework.
- Systematically monitors and studies the semi-annual data reports provided by obliged persons,
- Provides, when necessary, the necessary administrative assistance to supplement or correct the actions and practices of obliged persons.
- Records gaps in compliance with the regulatory framework.
- Collects information on the exclusive player accounts held by obliged persons with financial institutions, on the means of payment they use for making payments of bets and winnings to players and on how they are cleared. The above data is sent via appropriate channels to all involved bodies (IAPR, BoG, FIU).
- Collects information on the type of winning certificates issued by obliged persons to the beneficiaries (players).

²⁸³ Article 2(2) of HGC decision No. 129/2/7-11-2014

- Collaborates with public-sector bodies (FIU, Financial Police, Cyber-crime Unit etc.), providing the necessary administrative assistance and know-how within the remit of its competences.

The HGC's purpose is to achieve the maximum audit coverage of the field it is responsible for, by making optimal use of its human and material resources.

8.9.1.3. Availability and enforcement of administrative sanctions

Assessment Rating: Medium Low (0.4)

Article 52 of Law 3691/2008 provides for administrative sanctions in the event of non-compliance with the relevant provisions by obliged persons, which are assessed as particularly strict. It is noted, however, that until the issue of a relevant Regulation for the specialization of sanctions by offense and severity, the HGC cannot impose administrative sanctions for ML issues.

Finally, following the processing and study of the responses of providers organizing or conducting land-based gambling in the Greek Territory, to an anonymous questionnaire sent to them, to which five of the twelve providers responded, it was found that 100% (of respondents) are aware of the statutory administrative sanctions and believe that these would be imposed in case of non-compliance with the obligations set forth by Law 3691/2008.

8.9.1.4. Availability and enforcement of criminal sanctions

Assessment Rating: Medium (0.5)

Article 45 of Law 3691/2008 provides for the enforcement of criminal sanctions on obliged persons in the event of a deliberate failure to report a suspicious transaction (STR) or of sending false data, while also defining the criminal sanctions in the event of the offense of money laundering. Criminal sanctions are also provided for all the predicate offenses referred to in Article 3 of Law 3691/2008, either under the Criminal Code (criminal organization, terrorist acts and terrorist financing, bribery, trafficking in human beings, computer fraud, etc.) or under other provisions (e.g. Article 66 of Law 4174/2013 on tax evasion).

It is noted however that, pursuant to its establishment law, the HGC does not have the power to impose criminal sanctions.

Finally, 100% of providers who responded to the questionnaire stated that they are aware of the statutory sanctions for money laundering and terrorist financing, while 80% believe that they would be subject to criminal sanctions in case of non-compliance with the obligations set forth in Law 3691/2008.

8.9.1.5. Availability and effectiveness of entry controls

Assessment Rating: Close to Excellent (0.9)

The following are observed as regards the assessment criteria for this variable:

- The licensing process and conditions are clearly formulated in the relevant legislative and regulatory framework.
- There is in-depth knowledge, understanding and assessment of the risk of money laundering in gambling-related business/professional activities.
- During the licensing process, there are clear and effective control measures on the beneficial owner(s).

- The legislative framework for the licensing of land-based gambling providers is comprehensive and clear.

It is noted, however, that at the time when casino enterprises were licensed and the relevant right to organize and conduct other games of chance was granted to other providers, there were no relevant requirements for the implementation of preventive measures to combat money laundering.

8.9.1.6. Integrity of business/profession staff

Assessment Rating: High (0.7)

As regards the integrity of the staff of providers organizing or conducting land-based gambling in the Greek Territory, following the processing and study of their responses to an anonymous questionnaire they were sent, 80% (of respondents) stated that they had integrity control mechanisms for their staff on entry, and that their staff has integrity and does not cooperate in criminal activities or acts of corruption. In addition, 80% of the above responded that they have not observed any incidents of non-compliance with statutory obligations, omissions or negligence by their staff during the past five years. Finally, on a question as to whether they consider that there is a protection mechanism for themselves and their staff in cases of reporting suspicious transactions or other criminal activities to the Authority, 20% responded positively, 60% responded negatively and 20% chose not to respond.

The HGC is already in the process of finalizing the relevant regulatory framework and creating a control program on money laundering issues, which will enable it to collect data and verify the integrity of the providers' staff.

8.9.1.7. AML knowledge of business/profession staff

Assessment Rating: High (0.7)

According to the HGC's regulatory framework, obliged persons must take appropriate measures to ensure that the staff and the Physical Network (meaning all, and each separately, of the land-based points of provision of legitimate gambling services)²⁸⁴ are informed of the provisions of the Law, the Regulation and the policy for assessing the risk of money laundering and terrorist financing, by ensuring their participation in specialized training programs.

Regarding the knowledge of the staff of providers organizing or conducting gambling in the Greek Territory with a land-based network, on issues related to ML, it is noted that, following the processing and study of their responses to an anonymous questionnaire sent to them, 100% of respondents are aware of the procedures and obligations for compliance and reporting provided for by the relevant provisions, despite the fact that the same percentage responded negatively to whether they had attended educational programs on such issues.

Furthermore, it is noted that, on the basis of the responses provided, 80% of respondents stated that their staff were aware of the procedures and obligations for compliance and reporting of suspected incidents (including those subject to professional secrecy) provided for by Law 3691/2008, despite the fact that, in a similar question on staff training in related issues, the same percentage responded negatively.

²⁸⁴ Article 2(2) of HGC decision No. 129/2/7-11-2014

8.9.1.8. Effectiveness of compliance function

Assessment Rating: High (0.7)

With its decision No. 129/2/7-11-2014, the HGC specified the implementation of the provisions of Law 3691/2008 in the gambling sector and defined the obligations of obliged persons (with the exception of casino enterprises, for which a separate Regulation is being drafted).

On an administrative level, the HGC monitors and assesses the obligations of obliged persons on a regular basis, in order to directly intervene for taking further measures.

Tellingly, it is reported that only 25% of land-based gambling providers, who however account for almost 70% of the total turnover of the Greek land-based gambling market (five-year data series), have a recorded policy, duly approved by their board of directors and by the person in charge of the company's management in each case.

Following the processing and study of the responses to the relevant questionnaire, it is noted that 20% of respondents responded positively to whether they have designated an executive as compliance officer, 60% responded negatively, while 20% refused to respond. In a question on whether they have a compliance program that takes into account factors such as the client's country of origin, the volume and nature of the products provided and the client's trading profile, 80% responded negatively, while 20% responded positively.

However, it is worth noting that 40% of participants stated that they have rejected players who did not meet the statutory and regulatory requirements.

With regard to the conduct of internal and/or external audits on money laundering issues or the enforcement of disciplinary penalties in cases of violation of the company's compliance policy, respondents' responses differ significantly, with 40% of providers stating that internal audits are carried out on such issues, 40% responding negatively and 20% not responding at all. 20% of providers replied positively, that disciplinary penalties are imposed, 60% responded negatively and 20% did not respond at all.

8.9.1.9. Effectiveness of suspicious activity monitoring and reporting

Assessment Rating: High (0.7)

According to the FIU, in the 2011-2016 period, 59 reports of suspected transactions were submitted by providers organizing or conducting land-based gambling in the Greek Territory.

Three (3) of the twelve (12) above providers, who however account for almost 70% of the total turnover of the Greek land-based gambling market (five-year data series), have in their policies on combating ML/FT, documented procedures for keeping and storing documents and data related to compliance with legal requirements in related issues, and monitor trading relations and legal transactions with their clients in order to identify any unusual or suspicious transactions that could potentially be associated with ML/FT.

Finally, it is noted that 20% of providers who responded to the questionnaire responded that they have an IT system that facilitates the monitoring of their clients' transactions and compares them with their profile, serving in the effective identification and recording of all complex, unusually large and/or suspicious transactions, and that transaction logs are available in a format that facilitates the detection and tracking of cases of money laundering.

8.9.2. Inherent vulnerability (High)

The key factors affecting the inherent vulnerability of the Business/Profession are analyzed as follows:

8.9.2.1. Total size/volume of the business/profession

Assessment Rating: High

In total, there are 12 land-based gambling providers: 9 Casino enterprises, OPAP S.A., Hellenic Lotteries S.A. and Hellas Horse Races S.A.

Casino enterprises offer 2 categories of gambling: Table games and games of chance using gaming machines, while OPAP S.A. offers 3 categories of gambling: Number lotteries, Prediction Games and Games of chance played using gaming machines. Hellenic Lotteries S.A. offers 1 category of gambling: State Lotteries. Finally, Hellas Horse Races S.A. offers 1 category of gambling: Prediction Games.

The Gross Gain revenue of these providers for the year 2016 amounted to € 1,594,450,639.13, while for the last 5 years (2012-2016) they amounted to € 8,116,800,103.08. The companies of the OPAP Group (OPAP S.A., Hellenic Lotteries S.A. and Hellas Horse Races S.A.) account for 82% of the above total Gross Gain revenue for the last 5 years.

The Turnover of these providers for the year 2016 amounted to € 5,576,836,225.53, while for the last 5 years (2012-2016) it amounted to € 28,649,845,158.57. The companies of the OPAP Group (OPAP S.A., Hellenic Lotteries S.A. and Hellas Horse Races S.A.) account for almost 70% of the total turnover of the above providers for the last 5 years.

Finally, it is noted that land-based gambling providers account for around 54% of the total Turnover of Greece's gambling market, amounting to € 10,602,079,160.26 (year 2016).

8.9.2.2. Client-base profile of the business/profession

Assessment Rating: High

In the Greek territory, participation in gambling is allowed only to natural persons, in person and not through third parties. However, the lack of a list of Politically Exposed Persons, the inability to identify the players' country of residence (high-risk countries), the lack of knowledge about the origin of players' income, and the use of cash make the existing inherent risk high.

8.9.2.3. Level of cash activity associated with the business/profession

Assessment Rating: High

The vast majority of participations in land-based games of chance is made using cash.

Correspondingly, casinos pay out winnings almost exclusively in cash, while, for other land-based games of chance, the use of cash is allowed under certain conditions and up to certain levels of winnings.

8.9.2.4. Other vulnerable factors of the business/profession: Use of agents/intermediaries

Assessment Rating: High

Three (3) of the twelve (12) land-based gambling providers, who however account for almost 70% of the total turnover of the Greek land-based gambling market (five-year data series), use an extensive network of agents (physical network).

In any case, the strict regulatory requirements arising from the HGC's Regulation are also strictly applicable to the providers' physical network, while the responsibility for the continuous updating and training of the network agents on ML/FT issues lies with the obliged person.

8.9.2.5. Other vulnerable factors of the business/profession: Possible anonymous use of the product in the business/profession

Assessment Rating: Available

Except for casinos and gaming machines, in the majority of land-based games of chance, players participate anonymously. However, due diligence is applied and the player's name is registered when the winnings are collected, in accordance with the provisions of the legal and regulatory framework.

In casinos and games of chance conducted through gaming machines (VLTs), due diligence is applied when the Player enters the Provider's premises.

8.9.2.6. Other vulnerable factors of the business/profession: Difficulty in tracing the transactions

Assessment Rating: Easy to Trace

In land-based games of chance conducted with the use of individual player cards/electronic accounts, it is possible to trace transactions, irrespective of amount.

In land-based games of chance conducted without the use of individual player cards/electronic accounts, it is not possible to trace transactions/players, unless the transactions have been made via a financial institution (without use of cash). In particular, for Casino enterprises, which, as mentioned, represent, on a proportional basis, a small percentage of the Turnover of land-based gambling, the tracing of individual transactions/games is difficult, unless these have been made using the individual player cards/electronic accounts stated in the previous paragraph.

8.10. Online gambling

8.10.1. General variables

8.10.1.1. Comprehensiveness of anti-money laundering (AML) legal framework

Assessment Rating: Close to Excellent (0.9)

According to the assessment criteria for this variable, the online gambling market receives a high rating. This is due to the fact that the regulatory framework for the gambling market, based on Law 3691/2008 and HGC Decision No. 129/2/07.11.2014, hereinafter referred to as the Regulation, is very strict.

8.10.1.2. Effectiveness of supervision / oversight activities

Assessment Rating: Close to Excellent (0.9)

The supervision of obliged persons operating in the online gambling market as regards ML/FT issues can be rated as Close to excellent, as the HGC exercises, monitors and provides all that has been reported in the corresponding variable for the land-based network.

8.10.1.3. Availability and enforcement of administrative sanctions

Assessment Rating: Medium Low (0.4)

Article 52 of Law 3691/2008 provides for administrative sanctions in the event of non-compliance of the relevant provisions by obliged persons, which are assessed as particularly strict. However, until the issue of a relevant Regulation for the specialization of sanctions by offense and severity, the HGC does not impose administrative sanctions for ML issues.

Finally, it is noted that, following the processing of the responses by providers organizing or conducting online gambling in the Greek Territory to an anonymous questionnaire sent to them, it is noted that, of a total of twenty-two (22) providers questioned, 54.54%, i.e. twelve providers responded, stating that they are aware of the administrative sanctions provided for by law. It is worth noting that in a question about whether they believe that they would be subject to administrative sanctions in the event of non-compliance with the obligations under the provisions of Law 3691/2008, 83% of responders responded positively, while 17% negatively.

8.10.1.4. Availability and enforcement of criminal sanctions

Assessment Rating: Medium (0.5)

Article 45 of Law 3691/2008 provides for criminal sanctions for anyone responsible for money laundering operations. It is noted however that, pursuant to its establishment law, the HGC does not have the power to impose criminal sanctions. Its competence is limited to forwarding data and information concerning criminal offenses it becomes aware of to the competent judicial authorities.

Finally, 92% of providers organizing or conducting online gambling in the Greek Territory who responded to the questionnaire stated that they are aware of the criminal sanctions provided by the law for the prevention and suppression of money laundering, and that they believe they would be subject to criminal sanctions in the event of non-compliance with the obligations set forth by Law 3691/2008.

8.10.1.5. Availability and effectiveness of entry controls

Assessment Rating: Close to Excellent (0.9)

The following are observed as regards the assessment criteria for this variable:

- The licensing process and conditions are clearly formulated in Law 4002/2011.
- There is a good understanding and assessment of the risk of money laundering in these business/professional activities.
- During the licensing process, there are clear and effective control measures on the beneficial owner(s).

It is noted, however, that, until the issuance of the above licenses is approved, twenty-four (24) online gambling companies have been included in the tax regime provided for in Article 50(12) of Law 4002/2011, to be able to provide their services in the Greek territory, pursuant to Circ. No. 1248/2011. The prerequisites for the above companies to be included in the regime were their establishment and the possession of a legal license to provide online gambling from a European Union or European Economic Area country and the submission of a voluntary application to be included in the regime by 31.12.2011. Of these companies, 2 have been registered in the HGC's Blacklist.

8.10.1.6. Integrity of business/profession staff

Assessment Rating: High (0.7)

As regards the integrity of the staff of providers organizing or conducting online gambling, following the processing of their responses to an anonymous questionnaire they were sent, it was found that 100% of the twelve (12) providers responding to the questionnaire stated that they had integrity control mechanisms for their staff on entry, and that their staff has integrity and does not cooperate in criminal activities or acts of corruption. In addition, the above participants stated that, during the last five years, they have not observed incidents of non-observance of the obligations provided by the law on the prevention and suppression of Money Laundering/Terrorist Financing (Law 3691/2008) due to omissions or negligence of their staff.

Furthermore, on a question as to whether they consider that there is a protection mechanism for themselves and their staff in cases of reporting suspicious transactions or other criminal activities to the Authority, 60% of the above providers responded positively while 40% did not to respond.

Finally, the other ten (10) providers' failure to respond to the questionnaire is not affecting the above statistical result, as, in most cases, the failure to participate is linked to the fact that six (6) providers are inactive and one does not provide services due to not possessing a valid license.

8.10.1.7. AML knowledge of business/profession staff

Assessment Rating: High (0.7)

As regards staff knowledge on ML issues, 100% of responders stated that they are aware of compliance procedures and obligations, while 75% of providers have attended training programs on related issues.

8.10.1.8. Effectiveness of compliance function

Assessment Rating: Very High (0.8)

With its decision No. 129/2/07.11.2014, the HGC specialized the implementation of the provisions of Law 3691/2008 in the gambling sector and defined: 1) the obliged persons, 2) their obligations with regard to a) taking organizational measures (drawing up relevant policies, designation of a Compliance officer, staff education and training, monitoring of compliance); b) the implementation of due diligence measures; c) reporting to the FIU d) record keeping and 3) the procedure for carrying out compliance checks and taking corrective actions.

In addition, 92% of the providers who responded to the anonymous questionnaire sent replied that they have a compliance program in place, which takes into account factors such as the client's country of origin, the volume and nature of the services provided, the client's trading profile and the cross-border nature of the transactions. In addition, 91% of the above providers responded that they have rejected players who did not meet the statutory and regulatory requirements.

With regard to the conduct of internal and/or external audits on money laundering issues or the enforcement of disciplinary penalties in cases of violation of the company's compliance policy, all (100%) of respondents to the questionnaire responded positively, stating that they conduct audits, while 85% of respondents also responded positively that disciplinary penalties were imposed in cases of violation of the company's compliance policy.

Finally, it is worth noting that, based on HGC data, all providers of online gambling services have fully met the relevant regulatory requirement to designate a compliance officer for the combating of money laundering and terrorist financing.

8.10.1.9. Effectiveness of suspicious activity monitoring and reporting

Assessment Rating: Medium High (0.6)

Based on the HGC's records and the content of the biannual reports, online gambling providers implement measures and follow procedures and policies for the combating of money laundering. Furthermore, these reports provide information on the monitoring and reporting of suspicious and unusual transactions. In particular, it is reported that, by using information management systems, they approach, classify and assess the risks and, following a specific procedure, monitor any suspicious activities at all stages of the game until all collected information is evaluated.

Fifty per cent (50%) of respondents to the questionnaire stated that they have an IT system that facilitates the monitoring of their clients' transactions, the comparison of transactions with their profile, while helping to effectively identify and record all complex, unusually large and/or suspicious transactions. They also responded that transaction logs are available in a format that facilitates the detection and tracking of cases of money laundering.

8.10.2. Inherent vulnerability (Medium High)

The key factors affecting the inherent vulnerability of the Business/Profession are analyzed as follows:

8.10.2.1. Total size/volume of the business/profession

Assessment Rating: Medium High

As defined in Article 50(12) of Law 4002/2011, in the examined period, there were in total twenty-four (24) online gambling providers. It is noted, however, that, following an audit by the HGC, two (2) of them were included in its Blacklist. It is also noted that three (3) provider companies have declared to the competent tax office that they are inactive, while three (3) others state that they do not carry out any business activity in Greek Territory and remain inactive. Finally, one (1) provider company does not conduct any such business as it does not have a valid license.

The Gross Gain revenue of these providers for 2016 amounted to € 215,095,457.85, while their Turnover for 2016 amounted to € 5,025,242,934.73.

Finally, it is noted that online gambling providers account for around 46% of the total Turnover of Greece's gambling market, amounting to € 10,602,079,160.26 (year 2016).

As online gambling providers provide their services during the transitional period of Article 50(12) of Law 4002/2011, their financial information is based on their relevant statements to the HGC.

The HGC cooperates with the competent tax authorities to confirm that these are correct.

8.10.2.2. Client-base profile of the business/profession

Assessment Rating: High

In the Greek territory, participation in gambling is allowed only to natural persons, in person and not through third parties. However, the lack of a list of Politically Exposed Persons, the lack of knowledge about the origin of players' income, and the fact that players are not physically present at the gaming venue mean that the existing inherent risk is high.

8.10.2.3. Level of cash activity associated with the business/profession

Assessment Rating: Does not Apply

Pursuant to the regulatory framework, the use of cash is not allowed for online gambling.

8.10.2.4. Other vulnerable factors of the business/profession: Possible anonymous use of the product in the business/profession

Assessment Rating: Unavailable

According to the HGC's Regulation, players may not participate anonymously in online gambling. Players can participate only after their personal details are identified and verified, at the time when the client relationship is concluded.

8.10.2.5. Other vulnerable factors of the business/profession: Difficulty in tracing the transactions

Assessment Rating: Difficult/Time Consuming

Given that, as noted above, up to now, online gambling providers are established in countries of the European Union, any communication, cooperation and receipt of data/information becomes time-consuming and/or difficult.

8.10.2.6. Other vulnerable factors of the business/profession: Non-face-to-face transactions with the client

Assessment Rating: Available and Prominent

Transactions for players' participation in online gambling are conducted exclusively remotely. However, the legislative and regulatory requirements for strict adherence to due diligence measures adequately restrict ML/FT-related vulnerability factors, based on the players' participation method. Given the remote nature such games, online gambling entails vulnerabilities if the provisions of the HGC Regulation on the implementation of measures to combat money laundering are not adhered to.

8.11. Certified Auditors - Accountants

8.11.1. General variables

8.11.1.1. Comprehensiveness of anti-money laundering (AML) legal framework

Assessment Rating: Close to Excellent (0.9)

Based on the criteria of the variable, it was found that the AML legal framework is highly reliable and near-comprehensive in accordance with Law 3691/2008²⁸⁵.

Law 3148/2003 established the Hellenic Accounting and Auditing Standards Oversight Board (HAASOB), which is the supervisory body for chartered auditors-accountants, defined its responsibilities and regulated its operation. Law 4449/2017, which replaced Law 3693/2008, regulated issues relating to the statutory audit of annual and consolidated financial statements and the exercise of public oversight over

²⁸⁵ Articles 12-26, 29, 31, 33, 35, 41, 43 of Law 3691/2008

audits. Moreover, Regulation (EU) 537/2014 sets specific requirements for statutory audits of public-interest entities.

8.11.1.2. Effectiveness of supervision / oversight activities

Assessment Rating: Very High (0.8)

In accordance with article 6 of Law 3691/2008, the Competent Authority for supervising the implementation of the provisions of Law 3691/2008 by chartered auditors-accountants and audit firms is the HAASOB.

Supervision is exercised based on a clearly defined and comprehensive framework. There are documented inspection procedures for obliged persons, in the context of the quality control described in Law 3148/2003 as amended and currently in force, and in article 33 of Law No. 4449/2017.

In line with the obligations imposed by Law 3691/2008, the HAASOB issues regulatory acts, performs quality inspections through authorized auditors, makes recommendations based on quality inspections, conducts investigations to detect any breaches of the legislation and imposes administrative sanctions.

The HAASOB’s authorized inspectors understand the risks associated with money laundering and terrorist financing entailed in the profession of chartered auditors-accountants and are trained on such matters. Specifically, in October 2012, they participated in a seminar conducted by the Institute of Certified Public Accountants (ICPA) on policies and procedures for combating money laundering and terrorist financing.

The HAASOB has 6 authorized auditors for 46 audit firms in order to effectively audit the compliance of the persons it supervises with Law 3691/2008. However, its staff does not suffice to set up a special departmental unit with at least three full-time members of staff, as required by Law 3691/2008.

The HAASOB quality inspections are conducted following targeting²⁸⁶, based on specific criteria identified in the context of the risk assessment approach. On the HAASOB’s request, chartered auditors-accountants and audit firms send data on the statutory audits carried out and publish an annual transparency report on their website.

HAASOB Regulatory Act 004/2009 regulates the obligations of chartered auditors-accountants regarding the prevention and suppression of money laundering and countering the financing of terrorism, in accordance with the provisions of Law 3691/2008. Furthermore, Announcements 003/2012 and 002/2014 regulate the reporting obligations on the compliance of audit firms every two years.

Finally, the HAASOB keeps statistics of audits on adherence with due diligence measures, according to which the following quality audits were carried out on Chartered Auditors-Accountants during the last five years:

YEAR	NUMBER OF QUALITY CONTROLS
2012	9
2013	32
2014	17
2015	25

²⁸⁶ Announcement 001/2015 “CONDUCT OF QUALITY AUDITS FOR THE YEAR 2015” HAASOB

Table 57- HAASOB – Quality controls 2012-2016

The HAASOB records electronically the results of quality audits while the findings are presented in public annually. These records are used to extract data and formulate policies.

In view of the above, the effectiveness of the supervision of chartered auditors-accountants is considered Very High.

8.11.1.3. Availability and enforcement of administrative sanctions

Assessment Rating: Medium Low (0.4)

Article 52 of Law 3691/2008 as in force provides for corrective measures and/or administrative sanctions in the event of non-compliance by obliged persons with the obligations under Law 3691/2008, which are assessed as particularly strict. In addition, HAASOB Regulatory Act 4/2009 makes reference to the sanctions of Article 52 of Law 3691/2008.

However, the administrative sanctions provided for in Article 52 of Law 3691/2008 have not been enforced to date. In 2015, the HAASOB noted a violation of due diligence measures by a chartered auditor-accountant, which it communicated to the Authority.

A key reason for the non-enforcement of the stipulated administrative sanctions is the non-issuance of a Decision by the HAASOB, defining the degree of importance of each obligation, with an indication of the potential sanctions for non-compliance with such and other criteria for determining sanctions.

An additional difficulty in the enforcement of sanctions is that the sanctions provided for are particularly severe for chartered auditors - accountants who are freelancers, that is, they are natural and not legal persons.

Furthermore, 83% of the chartered auditors - accountants who responded to an anonymous questionnaire and, in particular, to the question of whether they are aware of the stipulated administrative sanctions, responded positively, while 87% believe that they will be imposed administrative sanctions in case of non-compliance with the obligations arising from the provisions of Law 3691/2008 and other regulatory acts.

Following quality audits it carried out pursuant to Law 3693/2008, the HAASOB imposed administrative sanctions, as provided by Law 3148/2003. Specifically, from 2013 to 2017, administrative sanctions (fines and/or temporary suspension of exercise of the profession) were imposed on a total of eleven chartered auditors - accountants and audit firms. Furthermore, in 2016, an audit firm had its license revoked due to formalities.

For all the other findings in of the quality inspections, recommendations were made to the audit firms and chartered auditors - accountants.

8.11.1.4. Availability and enforcement of criminal sanctions

Assessment Rating: Medium (0.5)

Article 45 of Law 3691/2008 provides for the enforcement of criminal sanctions on obliged persons in the event of a deliberate failure to report a suspicious transaction (STR) or of sending false data, while also defines the criminal sanctions in the event of the offense of money laundering. Criminal sanctions are also

provided for all the predicate offenses referred to in Article 3 of Law 3691/2008, either under the Penal Code (criminal organization, terrorist acts and terrorist financing, bribery, trafficking in human beings, computer fraud, etc.) or under other provisions (e.g. Article 66 of Law 4174/2013 on tax evasion).

Criminal sanctions are enforced by the competent Courts. However, the statistics of the Court Services do not record the occupation of the person on whom the criminal sanctions have been imposed; thus, no data are available on the criminal sanctions imposed on each category of obliged person, and consequently on chartered auditors-accountants, either for money laundering or for any other predicate or ancillary offense. Indications of the involvement of chartered auditors-accountants in the above criminal offenses arise only from reports in the press.

Finally, in the questionnaire, 87% of chartered auditors - accountants who responded stated that they were aware of the sanctions provided and believe they would be imposed on them.

8.11.1.5. Availability and effectiveness of entry controls

Assessment Rating: Close to Excellent (0.9)

Pursuant to the provisions of Article 3 of Law 4449/2017 as in force and Article 3 of Law 3693/2008, as was in force during the period 2012-2016, the HAASOB is the competent public authority for granting licenses to practice (professional licenses) to chartered auditors - accountants. Law 4449/2017²⁸⁷ and HAASOB Regulatory Act 003/2017 define the requirements and the procedure for granting licenses.

According to the HAASOB’s data, for the five-year period 2012-2016, the following applications were submitted for chartered auditor - accountant licenses, and the corresponding approvals and rejections were made by the HAASOB’s BoD:

YEAR	NUMBER OF APPLICATIONS	NUMBER OF APPROVALS	NUMBER OF REJECTIONS
2012	39	0	39
2013	52	25	27
2014	99	99	0
2015	159	142	17
2016	65	62	3

Table 58- HAASOB- Applications, approvals and rejections 2012-2016

²⁸⁷ Articles 5 and 7 to 11 and/or 13 of Law 4449/2017

8.11.1.6. Integrity of business/profession staff

Assessment Rating: Very High (0.8)

The profession of chartered auditor - accountant is governed by the Code of Ethics of the International Federation of Accountants (IFAC).

Article 5 of Law 4449/2017 stipulates the integrity of chartered auditors-accountants and their non-conviction by a final judgment of a penal court for certain offenses set forth in these provisions as a prerequisite for the granting of a professional license. Furthermore, Article 26 of Law 4449/2017 regulates all issues pertaining to the selection, evaluation and adoption of appropriate and effective organizational and management measures to prevent, detect, eliminate or manage and disclose any threats to the auditor's independence.

In accordance with the requirements specified in the International Standard on Quality Control (ISQC-1), each audit firm is required to maintain a system of controls regarding service quality and the compliance of its staff with the IFAC Code of Ethics.

Finally, in accordance with the International Standard on Auditing-220, the statutory auditor is responsible for implementing all procedures required to ensure that the audit team is fully compliant with the relevant ethical and independence requirements.

In the questionnaire, 100% of chartered auditors - accountants responded positively regarding the availability of a staff integrity control mechanism, and replied with certainty (100%) that their staff had integrity. Finally, 46% of chartered auditors - accountants responded positively regarding the existence of a staff protection mechanism in cases of suspicious transaction reporting to the Authority.

8.11.1.7. AML knowledge of business/profession staff

Assessment Rating: Very High (0.8)

The variable was first assessed in relation to the knowledge of the obliged persons themselves, namely chartered auditors - accountants, and then in relation to the knowledge of their employees. Questionnaires were used for both parameters.

Asked if they are aware of the procedures, compliance and reporting obligations provided by Law 3691/2008, the chartered auditors - accountants who replied answered positively with 91%. In the question on whether they had attended a training program to receive information about the legislation, policies and procedures in place to combat money laundering and terrorist financing, chartered auditors - accountants responded positively at a relatively high rate of 65%.

Further to Law 3691/2008, the HAASOB, with Regulatory Act No. 004/2009, notified chartered auditors - accountants of their obligation to inform their staff about ML/FT issues. In this context, the ICPA held a seminar on combating money laundering and terrorist financing.

According to the reports on the compliance function submitted to the HAASOB by the audit firms during the examined period, 20-25% of them reported that their staff had attended relevant in-house seminars.

In the question on whether their staff is aware of the procedures and obligations for compliance and reporting provided by Law 3691/2008, chartered auditors - accountants expressed certainty (100%).

In the question on whether their staff had attended a training program to receive information about the legislation, policies and procedures in place to combat money laundering and terrorist financing, chartered auditors - accountants responded positively at a relatively high rate of 69%.

Finally, in a relevant question, 82% of chartered auditors - accountants stated that their audit firms' training program and material relating to money laundering are adequate.

8.11.1.8. Effectiveness of compliance function

Assessment Rating: Very High (0.8)

Pursuant to Article 41 of Law 3691/2008, obliged persons must apply adequate and appropriate policies and procedures as regards due diligence to the client and the other obligations laid down by said law.

More specifically, for chartered auditors - accountants, with announcement No. 002/2014 "Submission of reports and data to the HAASOB", the HAASOB announced the obligation of the audit firms' compliance officers, arising from Article 6 of Regulatory Act 004/09, to submit to the HAASOB a detailed report of the audit firm's compliance function every two years.

In addition, the above Regulatory Act obliges the audit firms to designate a compliance officer, and also to regularly review their client acceptance policy, taking into account, inter alia, and the degree of risk for ML/FT.

In the question regarding the availability of a compliance program, 78% of chartered auditors - accountants responded positively. Meanwhile, 61% of chartered auditors - accountants responded that they have rejected clients because they did not meet the applicable compliance rules.

In the question addressed to chartered auditors - accountants who are legal entities as to whether internal audits on money laundering issues are conducted at their firm, 67% of those who completed the questionnaire responded positively. The question about undergoing external audits was addressed to those chartered auditors - accountants whose audit firms are members of a network. In this question, 60% of chartered auditors - accountants who completed the questionnaire responded positively. Regarding the enforcement of administrative sanctions against staff in case of violation of the company's compliance policy, 92% of chartered auditors - accountants responded positively.

8.11.1.9. Effectiveness of suspicious activity monitoring and reporting

Assessment Rating: Very High (0.8)

Pursuant to Article 26 of Law 3691/2008 and HAASOB Regulatory Act 004/2009, chartered auditors-accountants are obliged to inform the Authority without delay if they suspect a suspicious or unusual transaction.

Regarding the availability of an IT system for monitoring transactions with clients, 17% of chartered auditors - accountants who answered the questionnaire responded positively. Those who responded positively to the previous question stated with certainty that transaction logs are available in a format that facilitates the detection and tracking of cases of money laundering, while the system helps to effectively detect and record all complex and unusually large transactions, as well as suspicious transactions. Finally, 75% of the chartered auditors - accountants whose audit firms have a monitoring system in place stated that this helps to effectively identify politically exposed persons.

In a question of whether they are aware of the obligation to report suspicious transactions and activities to the Authority set by Law 3691/2008, 91% of chartered auditors - accountants were found to be

informed of this obligation. Meanwhile, chartered auditors - accountants stated with certainty (100%) that their staff are aware of this obligation.

According to the data of the Authority, in the period 2011-2017, chartered auditors - accountants submitted to it 123 reports of suspicious or unusual transactions.

8.11.2. Inherent vulnerability (Medium High)

The key factors affecting the inherent vulnerability of the Business/Profession are analyzed as follows:

8.11.2.1. Total size/volume of the business/profession

Assessment Rating: Medium High

According to the Public Register of Audit Firms and Chartered Auditors - Accountants kept at the HAASOB, in Greece, there are 46 audit firms and 1,210 chartered auditors - accountants, of which 845 are active (working in audit firms or independently).

Total revenue from audit services and other non-audit services for the three-year period 2014-2016, as emerging from the transparency reports of audit firms:

YEAR	REVENUE FROM AUDIT SERVICES	REVENUE FROM NON AUDIT SERVICES	TOTAL
2014	185.755.292	22.499.465	208.254.758
2015	193.615.076	8.788.726	202.403.801
2016	193.584.888	10.654.932	204.239.820

Table 59- Revenues 2014-2016

According to ICAP studies, over the past five years, chartered auditors - accountants are among the top 40 sectors of the Greek economy.

For all the above reasons, the size of the business sector, as compared to the rest of DNFBP businesses/professions, is considered Medium High.

8.11.2.2. Client-base Profile of the business/profession

Assessment Rating: High

The clients of chartered auditors - accountants are legal entities; this limits the vulnerability of this profession to high-risk clients, such as politically exposed persons. However, chartered auditors - accountants may provide their services to legal entities with a complex or opaque ownership structure, which makes it difficult to identify the beneficial owners.

In view of the above, the profile of the clients of chartered auditors-accountants is estimated to entail a High Risk.

8.12. Auction Houses

8.12.1. General variables

8.12.1.1. Comprehensiveness of anti-money laundering (AML) legal framework

Assessment Rating: Close to Excellent (0.9)

Based on the criteria of the variable, it was found that the AML legal framework is highly reliable and near-comprehensive in accordance with Law 3691/2008²⁸⁸.

In the context of informing the obliged persons in its remit - as the Competent Authority for auction houses - the IAPR's Directorate General of Tax Administration has issued decisions and circulars²⁸⁹ complementing and strengthening the legislative framework for combating money laundering and terrorist financing.

8.12.1.2. Effectiveness of supervision / oversight activities

Assessment Rating: Very Low (0.2)

Pursuant to Law 3691/2008, the Competent Authority for supervising the application of the provisions of Law 3691/2008 by auction houses is the IAPR's Directorate General of Tax Administration.

In the context of supervision, the Directorate General of Tax Administration periodically informs the obliged persons within its remit²⁹⁰, as well as the IAPR's auditors²⁹¹ by issuing documents, guidelines and manuals, either in writing or by posting them on the IAPR's website.

Furthermore, regarding the training of IAPR auditors and other officers, in the period from June 2012 to December 2013, 14 seminars were held in the framework of Technical Assistance to Greece in the field of money laundering and combating tax evasion. In addition, the training programs held for the IAPR's auditors from September - December 2013 included, inter alia, information on money laundering and terrorist financing issues.

Despite the above, there are serious weaknesses in the supervision of auction houses. The most important are the failure to update the policies and procedures regarding the supervision of obliged persons, the failure to issue recent manuals and instructions to auditors and the failure to carry out relevant inspections on auction houses over the past five years.

In view of the above, it is noted that there are serious weaknesses in the supervision of auction houses and thus the variable was rated as Very Low.

²⁸⁸ Articles 12-26, 29, 31, 33, 35, 41, 43 of Law 3691/2008

²⁸⁹ Circ. No.1185/2013, Circ. No.1067/2011, Circ. No.1196/2012, Circ. No DEL D 1191051 EX 2017/20.12.2017, Decision of the Minister of Finance 1051027/20340/ DE-E/20.04.2010 (GG B 605), Circ. No.1127/2010

²⁹⁰ Similarly to the previous footnote, as well as the FATF Public Statement and the results of its Plenary sessions (three times a year)

²⁹¹ IAPR Decision ΔΕΛ Δ 1117287 OUT 2013/23.07.2013, OECD manuals in Greek (Decision DEL D 1012476 EX 2013/22.01.2013 and Decision DEL E 1050451 EX 2015/17.04.2015 of the Audits Directorate), FATF Public Statement and the results of its Plenary sessions (three times a year)

8.12.1.3. Availability and enforcement of administrative sanctions

Assessment Rating: Low (0.3)

Pursuant to article 52 of Law 3691/2008, the Competent Authorities may impose corrective measures and/or administrative sanctions on obliged persons in the event of non-compliance with the obligations set forth by Law 3691/2008.

A key weakness is noted in the enforcement of administrative sanctions. The main reason for the non-enforcement of the stipulated administrative sanctions is the failure of the IAPR's Directorate General of Tax Administration to carry out the relevant inspections. Another important reason is the non-issuance of a Decision by the Competent Authority, defining the degree of importance of each obligation, with an indication of the potential sanctions for non-compliance with such and other criteria for determining sanctions.

A disincentive for the enforcement of sanctions is that the sanctions provided for are particularly severe for auction houses, given that the majority of them are small enterprises.

Finally, it is noted that auction houses do not appear to know the administrative sanctions provided for by the above law.

8.12.1.4. Availability and enforcement of criminal sanctions

Assessment Rating: Medium (0.5)

Article 45 of Law 3691/2008 provides for the enforcement of criminal sanctions on obliged persons in the event of a deliberate failure to report a suspicious transaction (STR) or of sending false data, while also defining the criminal sanctions in the event of the offense of money laundering. Criminal sanctions are also provided for all the predicate offenses referred to in Article 3 of Law 3691/2008, either under the Criminal Code (criminal organization, terrorist acts and terrorist financing, bribery, trafficking in human beings, computer fraud, etc.) or under other provisions (e.g. Article 66 of Law 4174/2013 on tax evasion).

Criminal sanctions are enforced by the competent Courts. However, the statistics of the Court Services do not record the occupation of the person on whom the criminal sanctions have been imposed; thus, no data are available on the criminal sanctions imposed on each category of obliged person, and consequently on auction houses, either for money laundering or for any other predicate or ancillary offense. Indications of the involvement of auction houses in the above criminal offenses arise only from reports in the press.

Finally, it is noted that auction houses do not appear to know the administrative sanctions provided for in the relevant legal framework.

8.12.1.5. Availability and effectiveness of entry controls

Assessment Rating: Close to Nothing (0.1)

Except for the registration of the interested person in the register of the competent Chamber and in the General Commercial Register (GCR), there is no relevant legislation regulating specialized issues of auction houses, with the exception of the conduct of auctions for movable monuments²⁹² in order to ensure the legitimate acquisition of the monuments by their owners or holders. In specific, the aforementioned Decision provides for the granting of a relevant license by the competent department of the Ministry of

²⁹² Decision of the Minister of Culture No. YPPO/DOEPY/TOPYNS/34674/11.04.2008

Culture, which is granted for a specific list of objects each time, as a prerequisite for conducting auctions for movable monuments.

8.12.1.6. Integrity of business/profession staff

Assessment Rating: Medium (0.5)

Despite not having a mechanism to control the integrity of their staff, both during recruitment and during employment at the company, auction houses state that they are confident about their integrity.

Finally, auction houses do not have a staff protection mechanism in cases of suspicious transaction reporting to the FIU.

8.12.1.7. AML Knowledge of business/profession staff

Assessment Rating: Close to Nothing (0.1)

No training seminars on money laundering addressed to auction houses and their staff have been organized by the Competent Authority for their supervision, i.e. the IAPR's Directorate General of Tax Administration.

The IAPR's Directorate General of Tax Administration has issued instructions to auction houses, as detailed in the variable concerning supervision, but these require updating. Furthermore, the information of auction houses becomes even more difficult due to the lack of a collective instrument, which would either inform its members voluntarily or forward the instructions issued by the Competent Authority to them.

The weaknesses in training in this business sector are in line with the low level of knowledge the auction houses' representatives stated as having as regards the procedures and obligations for compliance and reporting provided by the provisions of Law 3691/2008. In particular, when contacted, auction house representatives did not assess the risk of money laundering through their sector as high, given that the majority of transactions involve small amounts, and because transactions are mainly paid for using electronic payment instruments.

For all the above reasons, this variable is rated as Close to Nothing.

8.12.1.8. Effectiveness of compliance function

Assessment Rating: Close to Nothing (0.1)

Pursuant to Article 41 of Law 3691/2008, obliged persons must apply adequate and appropriate policies and procedures as regards due diligence to the client and the beneficial owner, and the other obligations laid down by said Law.

Despite the above obligation, auction houses do not have a compliance program, which is in line with their negligible level of knowledge in relation to combating money laundering and the weaknesses in their supervision.

It should also be noted that the provisions of Law 3691/2008, as well as other regulatory acts, do not provide for the obligation of auction houses to designate a compliance officer or to carry out internal audits. In this context, auction houses have not proceeded to the corresponding actions for designating a compliance officer or carrying out internal audits.

8.12.1.9. Effectiveness of suspicious activity monitoring and reporting

Assessment Rating: Close to Nothing (0.1)

Chapter F of Law 3691/2008 provides for the obligations of obliged persons in relation to record-keeping and the keeping of statistical data and information.

Auction Houses are not obliged to use an IT system to monitor transactions with their clients.

Regarding the sending of suspicious transaction reports, it is noted that despite the relevant obligation under article 26 of Law 3691/2008 and the instructions²⁹³ issued by the Directorate General of Tax Administration to obliged persons within its remit regarding the obligation to send reports to the FIU, when asked, auction houses stated that neither they nor their staff are aware of this obligation.

Meanwhile, the significant weaknesses regarding this variable are also evident from the fact that no STRs have been sent by auction houses to the FIU over the past five years.

Therefore, the variable is rated as Close to Nothing.

8.12.2. Inherent vulnerability (Medium)

The key factors affecting the inherent vulnerability of the Business/Profession are analyzed as follows:

8.12.2.1. Total size/volume of the business/profession

Assessment Rating: Low

The size of the auction house sector, as compared to the rest of DNFBPs, is considered Low, as this sector is not particularly developed in Greece and has shrunk even more in recent years due to the financial crisis.

Around 15 companies operate in this sector, most of which hold auctions on items of small value. Three companies are estimated to operate in the auctioning of higher value artworks, which hold two to four auctions per year. Some owners of high-value artworks who want to sell them prefer to contact foreign auction houses for this purpose.

8.12.2.2. Client-base profile of the business/profession

Assessment Rating: Medium

The clients of auction houses include natural persons from the entire spectrum of the economy, including high-net-worth individuals, Politically Exposed Persons, as well as clients with a criminal record or transacting with foreign countries. The frequency with which an auction house may have high-risk clients can only be estimated, as no statistics are available.

In view of the above, the profile of auction houses' clients is estimated to entail a Medium Risk.

8.12.2.3. Level of cash activity associated with the business/profession

Assessment Rating: Medium

With regard to the use of cash, auction houses are also subject to the tax legislation, i.e. the use of electronic payment instruments for transactions of over 500 Euro.

In recent years, online auctions, which mainly concern low-value items, have also been gaining ground. Online auctions do not use cash.

²⁹³Circ. No. 1067/2011, Circ. No. 1196/2012 and Circ. No. DEL D 1191051 EX 2017/20.12.2017 of the Audits Directorate

8.12.2.4. Other vulnerable factors of the business/profession: Non-face-to-face transactions with the client

Assessment Rating: Available and Prominent

Auction houses often transact with their clients via the internet, as they also hold online auctions, mainly for low-value items.

9. ASSESSMENT OF TERRORISM FINANCING IN GREECE

9.1. Introduction

For a more coordinated and effective national response to the threat of money laundering and terrorism financing, the "Strategy and Policy Assessment Committee to deal with money laundering and terrorism financing" was set up by the Ministry of Finance²⁹⁴. The work of the Committee is to prepare and design specific policies to address identified weaknesses in the country's general mechanism, in order to prevent money laundering activities and financing of terrorism, as well as the study and designing of the necessary legislative, regulatory and organizational measures to the extent of improving the supervisory framework and the country's compliance with international standards and requirements.

In this context²⁹⁵, the aforementioned Committee commissioned eight (8) Working Groups to implement the National Risk Assessment (NRA) for Money Laundering and Terrorism Financing. By Ministerial Decision of the Ministry of Finance was assigned to Working Group 8, the assessment of the risk and vulnerability of the financing of terrorism. This Working Group consists of fourteen (14) members representing the competent authorities for the fight against terrorism and its financing.

The Working Group used the World Bank's "National Risk Assessment Tool" and in particular the "Module 8-TFRiskAssessment.xls", the content of which is classified. The purpose of this tool is firstly to identify the threat of terrorism financing based on the threat of terrorism itself (proportionality), secondly the detection of the main threats of terrorism financing through the identification of its direction of financial flows, its sources and its networks and, finally processing the vulnerability of terrorism financing, based on the existing control mechanisms and the national factors that affect it. This tool includes the following sections:

1st section: *Terrorism Threat Assessment*

2nd section: *Terrorism Financing Threat Assessment*

3rd section: *Terrorism Financing Vulnerability Assessment*

After all the aforementioned modules, a detailed "Action Plan" was prepared in order to improve and ameliorate the current situation.

The above tool provided a suggested follow-up procedure for a reliable and unbiased estimation. As a period of research and collection of information were set the years between 2011 and 2016, including the current trends. Both qualitative (open sources, surveys, etc.) as well as quantitative (databases and statistics) indicators were used, as sources of the data and information gathered.

9.2. Terrorism financing assessment

Due to qualitative reasons, the general aspect of terrorism financing assessment was divided in two (2) sections, ("Domestic terrorism financing Assessment" and "International terrorism financing Assessment"). The overall aspect concerning financing of both Domestic and International terrorism is set at the "Medium - Low" level.

²⁹⁴ in accordance with article 9 of Law 3691/2008

²⁹⁵ in accordance with EU Directive 2015/849 as well as the FATF recommendations and the World Bank methodology

OVERALL DOMESTIC TERRORISM FINANCING ASSESSMENT						
OVERALL THREAT	HIGH	MEDIUM	MEDIUM	ΜΕΣΑΙΟ-ΥΨΗΛΟ	HIGH	HIGH
	MEDIUM - HIGH	MEDIUM	MEDIUM	MEDIUM – HIGH	MEDIUM – HIGH	HIGH
	MEDIUM	MEDIUM - LOW	MEDIUM	MEDIUM	MEDIUM – HIGH	MEDIUM - HIGH
	MEDIUM - LOW	MEDIUM - LOW	MEDIUM - LOW	MEDIUM	MEDIUM	MEDIUM
	LOW	LOW	MEDIUM - LOW	MEDIUM – LOW	MEDIUM	MEDIUM
		LOW	MEDIUM - LOW	MEDIUM	MEDIUM – HIGH	HIGH
OVERALL VULNERABILITY						

OVERALL INTERNATIONAL TERRORISM FINANCING ASSESSMENT						
OVERALL THREAT	HIGH	MEDIUM	MEDIUM	ΜΕΣΑΙΟ-ΥΨΗΛΟ	HIGH	HIGH
	MEDIUM - HIGH	MEDIUM	MEDIUM	MEDIUM – HIGH	MEDIUM – HIGH	HIGH
	MEDIUM	MEDIUM - LOW	MEDIUM	MEDIUM	MEDIUM – HIGH	MEDIUM - HIGH
	MEDIUM - LOW	MEDIUM - LOW	MEDIUM - LOW	MEDIUM	MEDIUM	MEDIUM
	LOW	LOW	MEDIUM - LOW	MEDIUM – LOW	MEDIUM	MEDIUM
		LOW	MEDIUM - LOW	MEDIUM	MEDIUM – HIGH	HIGH
OVERALL VULNERABILITY						

9.3. Terrorism threat assessment

9.3.1. Domestic terrorism

9.3.1.1. Far left wing – Anarchist terrorism

The main threat for our country derives from Domestic terrorism. The terrorist groups that act in the Greek territory are inspired by far left-wing and anarchist ideology. During the period 2011-2017, several terrorist attacks executed by the abovementioned groups, nevertheless most of them considered to be of low power. Members of the aforementioned terrorist groups alleged to have a spirit of "nihilism" that led them to turn against symbolic targets in order to provoke public protest and establish revolutionary impetus. In this manner, they tend to express their rejection of the sovereign values of society. Potential targets of these groups, are mainly representatives and infrastructures of justice, police, economic and diplomatic interest. It has been monitored that currently active terrorist groups, mainly those that inspired by anarchist ideology background, linked to individuals or gangs of common criminal law or organized crime. In this way terrorist groups have access to certain criminal links from where they can acquire weapons and explosive materials in order to supply and upgrade the capabilities of their

organization. The main source of subsidizing their own illegal activity and terrorist acts, derives from bank robberies.

The Counter-Terrorism Unit's (C.T.U.) repressive action, in terms of numerous arrests of both leading and other members, has resulted in domestic terrorist organizations that have gained upgraded action in recent years to suffer major hits. Thus, it is estimated that the terrorist groups operating within the Greek territory are going to limit their activity. Additionally, persistent & unremitting efforts and investigations are being made by the Law Enforcement Authorities to identify and arrest other involved members of terrorist organizations. At the same time, arrested members of the terrorist groups have posted some texts at specific websites inspired by anarchist ideological background. The main topics of these texts related to reorganization - rebuilding of the "urban guerilla" while in some others prevail the idea of armed struggle revival. Despite authors' strenuous effort to radicalize and recruit some individuals who aspire left-wing & anarchist ideology, it does not seem to have great impact, since the above arrests considered to be a deterrent factor of undertaking operational action.

Last year (2017), some cases of sending parcel-bombs (trapped with Improvised Explosive Devices) not only in the Greek territory but also abroad re-emerged. Recipients of the above mentioned parcel-bombs were individuals of economic - political - judicial interest. This operational methodology (modus operandi) results in an operational reorientation of domestic terrorist groups, allegation which supported by the fact that some parcel-bombs arrived in the country of final destination.

At the beginning of the year 2017, quick response was given by Greek Counter-Terrorist Unit (C.T.U.) which arrested two (2) individuals - members of an active terrorist group. Specifically, one of them was a leading member of an active terrorist group. These arrests, alleged to be a crucial factor in terms of dismantling the operational capacities of the above mentioned terrorist group and as a result discontinue its activity. Furthermore, in the second semester of 2017, Greek Counter-Terrorist Unit (C.T.U.) under rigorous investigations came up to another individual. This individual was arrested for being involved in the cases of sending parcel bombs in Greece and abroad.

Taking into consideration all the data above, the level of threat posed by Far Left Wing & Anarchist Terrorism is classified as medium-low.

9.3.1.2. Far right wing terrorism

Till now, no terrorist activity by far Right-Wing groups has been reported. However, the socio-economic situation in Europe, coupled with the migratory / refugee crisis and the rise of jihadist terrorism, have created a solid ground for rising far right-wing rhetoric and extremist activity both in Europe and in our country.

The level of threat posed by far Right-Wing terrorism is currently low.

9.3.2. International terrorism

9.3.2.1. Religiously motivated terrorism

In recent years EU and generally global community face a number of terrorist attacks most of which are related to religious motivated terrorism. The implementation of these plots is undertaken by both jihadist organized cells and networks as well as by individual terrorists. Recent attacks have shown that terrorists are targeting the greatest possible number of victims, mostly defenseless and unsuspecting citizens in public places.

Concern is also raised, about the choice of "soft" targets and simple citizens and vital infrastructure by terrorists, the use of sophisticated tools for their communications, the use of the Internet and social media for recruitment and other purposes, the engagement of social networks with different socio-cultural characteristics (citizenship, educational level, participation in criminal / terrorist activities) in terrorist activity, as well as the presence of persons within the European territory who have either returned from war zones, or had expressed an interest in going to these zones but for some reason their journey was cancelled. At the same time, the risk is rising even further, as it appears that the organization and preparation of most terrorist attacks, takes place within European territory, with interconnections and with support networks in other countries.

However, the competent Greek authorities are vigilant, taking into account the diffusion of terrorist attacks inside and outside the EU. The risk of possible exploitation of migratory / refugee flows by members of extremist / terrorist groups remains obvious. The identification of people returning from conflict zones, whether they are citizens of the EU or third countries is a major challenge for all European authorities. International terrorism, with its predominantly jihadist expression, does not appear to pose a serious threat to our country. The absence of intelligence indicating a terrorist activity from a network or an individual, the non-direct targeting of the country, the occasional nature of the arrests of individuals with suspect activity linked to jihadi terrorism in our country, sets the level of the threat (medium-low).

9.3.2.2. Non-Religious motivated terrorism

Relevant investigations regarding a political motivated international terrorist organization have inferred the absence of specific motivation for conducting attacks in our country, the lack of indications of a continuous illegal action within Greek territory, in parallel with the number of terrorists' arrests in previous years and recently, minimize the threat.

Therefore, the level of threat from non-religiously motivated terrorism is low.

9.3.3. Terrorist Financing threat assessment

The operational activity of terrorist groups is inextricably linked to their ability to finance their terrorist attacks. In this issue, the implementation of various ways in order to obtain financial resources is considered to be an important factor. Obtaining the necessary funds claimed to be a crucial factor for the terrorist groups so as to achieve both their strategic and operational goals.

9.3.3.1. Domestic terrorism financing

The operational activity of domestic terrorist groups is based on the preparatory acts of terrorism, such as armed robberies, prominent thefts of cars and forgeries of identification documents. The main source of funding their attacks is considered to be armed robberies of financial institutions across the Greek territory. It has been detected that some of them, had been committed in collaboration with individuals related to organized crime. This cooperation was not necessarily on the basis of ideological motivation, but on the achievement of a common purpose with criminal characteristics.

The funds collected by the robberies used to cover the cost of living of members of terrorist groups and upgrade their operational capacities through the acquisition of weapons and explosive materials. In order to meet these needs, money is transferred in cash from one member to another, avoiding, in this way, the use of the financial system (Banking sector & other Financial Institutions). According to the in-depth analysis that has been conducted concerning the use of counterfeit documents in terrorists' transactions, through the financial system, no findings came up.

Concerning terrorist financing issues, as well as terrorist attacks, till now, no links have been detected between members of domestic terrorist groups with individuals or other groups operating abroad.

In the time span, there has been no arrest - conviction of individuals about terrorism financing provisions of the Greek Penal Code, however, some persons associated with terrorist activity have been convicted of armed robberies. It is worth mentioning that some of the above cases have been referred for a judicial inquiry into terrorist financing and money-laundering offenses. Finally, the numerous arrests of members of terrorist groups and the seizure of a large amount of money have resulted in inducing great "damage" regarding their financial resources.

Taking into consideration all the above data, the level of threat posed by financing of domestic terrorism is currently medium-low.

9.3.3.2. International terrorism financing

Financing international terrorism varies according to the modus operandi of each terrorist organization. Regarding general findings of the competent authorities, the main pattern is the transfer of small amounts of cash through persons without a known criminal record, to avoid the restrictions set by the banking sector. It is noted that the role of these persons is often limited to the money transfer, as they have no other active role in the group. The financial sector (money remitters and money transfer companies) appears to be rarely used as means of transferring money. However, occasionally low-value transfers have been observed through money remitters.

As a result of investigations and evaluation of relevant information by the competent authorities, no evidence was found for the financing of jihadist terrorism in Greece.

Authorities are also aware of the potential use of informal money transfer systems using the "hawala" method, which has been observed internationally. Till now, there is no evidence that informal money transfer systems are associated with terrorist financing in our country.

To prevent the financing of terrorism, the authorities are taking into consideration the potential involvement of non-profit organisations that are active in the Greek territory, especially in areas where a large number of migrants and refugees are hosted, although no evidence has emerged.

The level of the threat to the financing of international terrorism is currently low.

9.3.4. Terrorism financing vulnerability assessment

Fighting against terrorism and its financing is a paramount priority for Greece in both national and international level. This is obvious not only by the continuous initiatives and actions in this field but also by the progressively targeted orientation of the responsible authorities on issues of terrorism financing.

In the context of the implementation of international and European treaties, the Greek legal framework criminalizes the act of terrorism financing and at the same time provides the authorities with a strong "legal weapon" to deal with the above crime. Moreover, the experience of professionals of the relevant agencies and their high level of expertise contribute effectively in countering this phenomenon. The appointment of Prosecutor for Terrorism Issues and his close cooperation with the President of the "Anti-Money Laundering Counter-Terrorist Financing and Source of Funds Investigation Authority", Deputy Prosecutor of the Supreme Court of Greece, contribute drastically to the effectiveness of the researches in financing of terrorism.

It is worth mentioning that any information of judicial proceedings is directed to a Central Service (C.T.U.), and thus their segregation is avoided and their exploitation is optimized. Nevertheless, the cooperation

and coordination between the competent authorities at both national and international level on counter terrorism financing issues is considered to be effective and dynamically evolving.

Finally, as Greece recognizes its vulnerability resulting from its geographical position, uses a significant number of national resources in cooperation with international and European institutes, not only for the control of its borders but also for the management of mixed migration flows.

However, the extensive study of different variables pointed out weaknesses which affect the overall vulnerability of the country in financing of terrorism. The pending issues regarding to the country's legislative transposition with international and European legal instruments and the non-timely implementation of legislation (issuance of Joint Ministerial Decisions) about issues related to terrorism and terrorism financing, affect the effectiveness of monitoring and limiting the phenomenon.

Furthermore, the insufficient number of experts on countering terrorism financing within the Law Enforcement Agencies and the Authority of the art. 7 of L. 3691/2008 and the further familiarization of representatives of the judicial and prosecutorial authorities in dealing with such cases increase the country's vulnerability.

Furthermore, deficiencies on issues concerning administrative and digitalization procedures in some entities of public sector is a crucial issue in retrieving data and information for the extraction of valid conclusions. Additionally, the establishment of a central registry/database for all the non profit organisations might contribute in the field of regular inspections by nominated authorities.

Finally, the further evaluation and in-depth analysis of the potential use of informal money remittances in terms of possible establishment of legislative/regulatory framework could assist in the amelioration in the overall spectrum of financial flows monitoring.

Taking into account all the aforementioned, the level of terrorism financing vulnerability of Greece is medium-low.

ANNEXES

I. THREATS

Annual Report 2015-2016 Corruption Data Collection Presentation (Prosecutors) General Secretariat for Combating Corruption The General Secretariat for Combating Corruption has made a great effort to gather and exploit evidence for corruption cases through the criminal justice system. In particular, the General Secretariat for Combating Corruption carried out an investigation with data collected from a sample of 80% of local Court of First Instance Prosecutors and the Athens Prosecutor's Office against Corruption. Data collection and processing took place between April and May 2016.

OFFENCE	NATURE OF THE OFFENCE	NUMBER OF PROSECUTIONS / NUMBER OF DEFENDANTS 2014	NUMBER OF PROSECUTIONS / NUMBER OF DEFENDANTS 2015
Political officials accepting bribery	Felony	0	0
Bribing political officials	Felony	0	0
Negligent failure to prevent bribery of officials	Misdemeanour	0	
Employee accepting bribery (misdemeanour)	Misdemeanour	13/19	8/13
Employee accepting bribery (felony)	Felony	25/230	17/222
Employee bribery (misdemeanour)	Misdemeanour	17/179	9/43
Employee bribery (felony)	Felony	17/68	7/183
Bribery of/Acceptance of bribery by foreign public officials and international organisation officials etc.	Felony/Misdemeanour (as applicable)	2/43	1/2
Request or acceptance of unlawful provision by an employee	Misdemeanour	0	1/1
Negligent failure to prevent bribery of an employee	Misdemeanour	0	0
Negligent failure to prevent acceptance of bribery	Misdemeanour	0	0
Acceptance of bribery by a	Felony	0	0

judge			
Bribery of a judge	Felony	0	0
Negligent failure to prevent bribery of a judge	Misdemeanour	0	0
Influence peddling/intermediaries	Misdemeanour	0	1/1
Bribery/Acceptance of bribery in the public sector	Misdemeanour	0	1/1
Breach of trust with respect to the service (misdemeanour)	Misdemeanour	16/92	17/56
Breach of trust with respect to the service (felony)	Felony	70/320	52/395
Embezzlement with respect to the service (misdemeanour)	Misdemeanour	51/67	37/44
Embezzlement with respect to the service (felony)	Felony	40/57	25/34
TOTAL		251/1,075	176/995

SMUGGLER'S ARRESTS		
NATIONALITY	2015	2016
Greece	257	207
Syria	319	161
Albania	179	111
Pakistan	189	96
Turkey	44	86
Bulgaria	100	68
Afganistan	63	41
Ukraine	74	26
Iraq	48	17
Georgia	18	13
Other	210	124
TOTAL	1501	950

II. NATIONAL VULNERABILITY

ΠΙΝΑΚΕΣ 1-3 : LEGAL FRAMEWORK FREEZINGS, SEIZURES CONFISCATIONS

TABLE 1

SEIZURE PROVISIONS			
S/N	LEGISLATIVE PROVISION	CRIMES FOR WHICH IT IS IMPOSED	WHEN IMPOSED
1.	Art. 243, Criminal Procedure Code	Caught in the act (Felonies and misdemeanors)	Article 243 requires investigating officers to conduct investigative measures such as seizures when an offence has been committed or the perpetrator is arrested in the act of committing the offence. After the seizure has taken place, the investigating officer must immediately notify the prosecutor who will determine the further actions.
2.	Art. 260 and following, Criminal Procedure Code	Felonies and misdemeanors	The persons referred in Art. 251 may seize securities in banks or other public or private institutions in amounts deposited in a current account and any other deposited stuff or document and when contained in security boxes even if they do not belong to the accused provided that they are related to the crime..
3.	Art. 147, Law 2960/2001- Customs Code		Art 147 provides that the custom authority may freeze the cash holdings of more than 10.000 € which enter or departure from the EU and have not been declared in accordance with Art. 3 of Regulation 1889/2005. The investigation can not last for more than three months after the freezing.
4.	Art. 2 (2) , Law 4312/2014	Lift of seizure	Article 2 (2) provides that if the suspect or accused, voluntarily consents to the payment of the amount initially to the Grec State, further seizure of his property is lifted.

TABLE 2

ASSET FREEZING PROVISIONS						
S/N	LEGISLATIVE PROVISION	COMPETENT AUTHORITY	MEASURE TYPE/PURPOSE	WHEN IMPOSED	CONTENT OF ASSET FREEZING	POSSIBILITY OF APPEAL - LIFTING CONDITIONS
1.	Art 46(5), Law No. 4174/2013 - Tax Procedure Code (as clarified by POL 1282/2013- Measures of public interest for the prevention of tax evasion and cases of its lifting, based on a. 46, Law 4174/2013)	Tax Administration	An immediate and emergency preventive administrative measure , aiming to safeguard public interest.	Based on a Special Audit Report, if the Tax Administration finds non-performance, inaccurate performance, offsetting, deduction or holding of VAT, Turnover Tax, tax on premiums, withheld, imposed taxes, fees and levies for the purpose of non- payment of a total amount of more than 150,000 € to the State, as well as the recovery of the above taxes after misleading the Tax Administration by presenting false facts as true or by unlawfully ignoring or hiding real facts.	The Tax Administration may not receive or deliver documents required for the transfer of assets. In this case, fifty per cent (50%) of deposits, from all kinds of accounts and deposits and the contents of the deposit boxed of the liable offender shall be frozen. Non-cash contents of deposit boxes and non-cash deposits shall be frozen in their entirety.	Art. 5 of POL 1282/2013 provides for an administrative appeal and a request to suspend the application of the measures before the Internal Re-examination Service under a special administrative procedure. Art. 6 POL 1282/2013 provides for cases of total or partial lifting of the measures.
2.	Art. 153, Law 2960/2001- Customs Code	Customs Authority	An immediate and emergency preventive administrative measure , aiming to safeguard public interest.	When a Customs Authority detects smuggling or fraud which, based on a Special Audit Report, show that more than 150,000 € of duties, taxes, and other charges have evaded and have not been delivered to the State or the EU.	It is forbidden for the competent Tax Authorities to receive statements or to issue the reports or certificates required by the applicable provisions and requested by the offender for the preparation of notarial deeds for the transfer of assets. In this case, the confidentiality of deposits, accounts, joint accounts, contracts and transactions in derivative financial products and the content of the offender's deposit boxes in Banks or other Credit Institutions is suspended with respect to the State and 50% thereof is frozen.	Art 153(4) of Law 2960/2001: Possibility to apply to the Minister of Finance for the total or partial lifting of the measures. An appeal against the decision of the Minister is permitted under the Code of Administrative Procedure. Art 153(5) of Law 2960/2001 provides for a mandatory principle of measures.

3.	Art. 30(5), case e of Law 3296/2004 (this provision has been found to be contrary to the Constitution by decisions 3316/2014 and 1260/2015 of the Council of State)	Special Secretariat of the Financial and Economic Crime Unit	An administrative measure , aiming to safeguard public interest.	In special cases of safeguarding public interest or in cases of financial crimes and illicit trade.	Bank accounts and assets are bound by a letter from the head of the competent Regional Directorate, informing the competent Prosecutor about this action within a 24-hour period.	In the absence of a specific provision, the appeal provided by the Code of Administrative Procedure may be exercised. No conditions and procedure for lifting the measures are foreseen.
4.	Art. 17A, Law 2523/1997 - Economic Crime Prosecutor	Economic Crime Prosecutor and assistant prosecutor officers	A measure taken in the framework of a preliminary criminal investigation .	In the event of a criminal investigation being carried out to ascertain the occurrence of any kind of tax and economic crime and any other related ones, if these are committed to the detriment of the Greek State, local authorities, public law entities, legal entities of the wider public sector and the EU or if they seriously harm the national economy.	By reasoned order, the Prosecutors undertake to freeze bank accounts, deposit box contents and property assets in general, real estate and movable assets for a period of up to one year (the period may be extended by a decision of the Council of Court of Appeals Judges of Athens or of the Council of Misdemeanour Court Judges of Athens)	Appeal possible before the Council of Court of Appeals Judges of Athens or of the Council of Misdemeanour Court Judges of Athens
5.	Art 2(6) of Law 4022/2011- Hearing of corruption cases of politicians and state officials, cases of major social interest and major public interest and other provisions	Examiner of Corruption Crimes	A measure taken in the framework of a preliminary criminal investigation .	Where there are reasonable grounds for believing that the accounts, securities, financial products or deposit boxes contain money or property proceed from the commission of an investigated crime.	Upon the prosecutor's agreement the trial examiner prohibits the movement of any type of accounts, securities or financial products held at a credit institution or financial institution and the opening of any safe deposit box kept by the defendant, even joint ones with any other person.	Right to request the removal of the trial examiner's order to the judicial council

6.	Art. 48, Law 3691/2008 - Prevention and suppression of money laundering and terrorist financing and other provisions	Examiner or Judicial Council	A measure taken in the framework of preliminary examination, preliminary investigation or preliminary examination.	<p>1. When a regular examination or preliminary investigation or preliminary examination is carried out on money laundering and terrorist financing offences as defined in Article 2 of the Law and there are reasonable grounds for believing that the accounts, securities, financial products or money or property proceed from committing an investigated crime.</p> <p>2. When an interrogation or preliminary investigation is conducted for a predicate offence as defined in article 3 of the Law and there are reasonable grounds to suspect that the accounts, securities, financial products or safe deposit boxes contain moneys or things resulting from committing the above crime and are subject to confiscation.</p>	Upon the prosecutor's agreement the trial examiner prohibits the movement of any type of accounts, securities or financial products held at a credit institution or financial institution and the opening of any safe deposit box kept by the defendant, even joint ones with any other person. The trial examiner may also order the prohibition of sale for a specific property of the defendant. In the event of a preliminary investigation or investigation, the prohibition of movement of accounts, securities, financial products or the opening of safe deposit boxes can be ordered by the judicial council.	Right to request the removal of the trial examiner's order to the judicial council
7.	Art 48(5) of Law 3691/2008 - Prevention and suppression of money laundering and terrorist financing and other provisions	President of the Anti-Money Laundering, Counter-Terrorist Financing and Source of Funds Investigation Authority		When the Authority's Unit A is conducting an investigation.	Prohibition of movement of accounts, securities and financial products, of opening deposit boxes and transferring or selling any assets.	Right to request the removal of the trial examiner's order to the judicial council

8.	Art. 3, Law 2655/1998 - Ratification of the European Convention on Laundering, Search, Seizure and Confiscation of the Proceeds from Crime	Judicial authority	A measure taken in the framework of a criminal pre-trial procedure	Following proceedings relating to one or more criminal offences	The Member-party adopts those laws and other measures it deems necessary to recognise and search for confiscated assets and to prevent any transaction, transfer or disposal of such assets.	
9.	Art. 11, Law 2655/1998 - Ratification of the European Convention on Laundering, Search, Seizure and Confiscation of the Proceeds from Crime (Chapter III International Cooperation)	Judicial authority	A measure taken in the framework of a criminal pre-trial procedure	At the request of another Party which has initiated criminal proceedings or confiscation procedures	The other Party (Greece) shall take the necessary interim measures, such as a ban on the opening of accounts or seizure, to prevent any action, transfer or disposal of any asset that could subsequently be the subject of a confiscation order or which could allow the satisfaction of such an order.	

10.	Art. 1, Law 4478/2017 Ratification and adaptation of the Greek legislation to the Warsaw Convention of 16th May 2005 of the Council of Europe, CHAPTER II, art. 2 and CHAPTER III, art. 3, 5, 6	Court or other competent authority			Each Party shall ensure that it is able to investigate, identify, determine, freeze, seize assets of legitimate or illicit origin that have been used or have been made available for use by any means, in whole or in part, to finance terrorism or products of that offence	
11.	Art. 7 Directive 2014/42/EU on the freezing and confiscation of instrumentalities and the proceeds of crime in the European Union				Member States shall take the necessary measures to allow the freezing of assets for possible subsequent confiscation.	
12.	Article 2(2), Law 4312/2014		Lifting of the Freezing			Article 2 par. 2 stipulates that if the suspect or accused voluntarily agrees to pay the amount that was initially the object of the freezing or seizure to the Greek State, the freezing or seizure is lifted.

TABLE 3

CONFISCATION PROVISIONS			
S/N	LEGISLATIVE PROVISION	CRIMES FOR WHICH IT IS IMPOSED	ASSETS CONCERNED
1.	No. 160, Law 2960/2001- Customs Code	Smuggling	1. Goods affected by smuggling 2. Animals, carriages, vehicles, ships of any capacity, logistic vessels engaged in virtual supplies and any other means of transport used for the transport of the object of smuggling of goods
2.	Art. 46, Law 3691/2008 - Prevention and suppression of money laundering and terrorist financing and other provisions	1. Money laundering and terrorist financing 2. Predicate offences, as stipulated in art. 3 of L. 3691/2008	Assets that are products of such offences or acquired directly or indirectly by the proceeds of such offences or the means used or intended to be used to commit the offences. In the event that the above assets or products no longer exist, have been found or cannot be seized, assets of equal value are seized and confiscated.
3.	Art. 76 of the Criminal Code	A felony or a misdemeanour, which stems from deceit	Object or assets that are the proceeds of such offences, as well as their price and those acquired directly or indirectly from them, as well as objects or assets which served or were intended to serve to perform such an act
4.	Art. 238 of the Criminal Code	Employees accepting bribery, employee bribery, court officials accepting bribery and bribery of court officials, influence peddling, accepting bribery and bribery in the private sector	Bribes and any other assets given, as well as those acquired directly or indirectly by them.
5.	Art. 1, Law 4478/2017 Ratification and adaptation of the Greek legislation to the Warsaw Convention of 16th	Money laundering and offence categories in the annex to the Convention, terrorism financing	Art. 1, Law 4478/2017 Ratification and adaptation of the Greek legislation to the Warsaw Convention of 16th May 2005 of the Council of Europe, on Laundering, Search, Seizure and Confiscation of the Proceeds from Crime and on the Financing of Terrorism

	May 2005 of the Council of Europe, on Laundering, Search, Seizure and Confiscation of the Proceeds from Crime and on the Financing of Terrorism		
6.	Art. 4-6 Directive 2014/42/EU on the freezing and confiscation of instrumentalities and the proceeds of crime in the European Union	<ol style="list-style-type: none"> 1. active and passive bribery in the private sector 2. offences relating to participation in a criminal organisation, 3. recruiting a child to participate in pornographic performances, etc. 4. illegal system interference and illegal data interference, 5. a criminal offence punishable by a custodial sentence of at least 4 years, in accordance with the relevant national law. 	Art. 4-6 Directive 2014/42/EU on the freezing and confiscation of instrumentalities and the proceeds of crime in the European Union

Memorandum of Understanding (MoUs) by the AML/TF Authority

Memorandum of Understanding (MoUs)	
Countries	Year
PANAMA	2015
ISRAEL	2015
LEBANON	2014
GEORGIA	2014
AUSTRALIA	2013
PHILLIPINES	2012
ALBANIA	2012
RUSSIA	2012
UKRAINE	2012
UNITED ARAB EMIRATES	2010
ARGENTINA	2010
SERBIA	2009

SINGAPORE	2005
ITALY	2002
ROMANIA	2002
FRANCE	2000
BELGIUM	1999

III FINANCIAL CRIMES INVESTIGATION AGENCIES

Enforcement/Controlling Authorities	Responsibilities
S.S. of the F.E.C.U. Special Secretariat of the Financial and Economic Crime Unit	Managed by the Ministry of Finance, it conducts investigations and controls to identify, document and repress economic crimes ²⁹⁶ in order to protect the interests of the Greek State and the EU without having any tax and customs responsibilities ²⁹⁷ .
I.A.P.R. Independent Authority for Public Revenue	Founded on 01/01/2017 ²⁹⁸ (replaced the General Secretariat for Public Revenues). It enjoys operational independence, administrative and financial autonomy and is subject to parliamentary scrutiny. The new framework of its organisational structure and operation includes identifying and combating tax evasion, smuggling, tax fraud, corruption.
Economic Crime Investigation Directorate	The Economic Crime Prosecutor manages and coordinates the Service's operation. Its mission is solely to carry out investigations, preliminary inquiries or preliminary examinations to verify that a major criminal tax offence ²⁹⁹ and any other perfectly related economic crimes that seriously damage the interests of the Greek State and the European Union have been committed, upon the order of the Economic Crime Prosecutor or his deputy or assistant prosecutors, under the supervision of the Economic Crime Prosecutor.
Hellenic Police	Its primary mission is the prevention and repression of crime. The detection and investigation of predicate offences and, by extension, money laundering are carried out by all Police Services in the territory, as well as by specialised Police Services ³⁰⁰ , as follows: Economic Police Directorate, whose mission ³⁰¹ is the prevention, investigation and repression of economic crimes against the financial interests of the State and the national economy, having the characteristics of organised crime. It is the competent police

²⁹⁶ P.D. 142/2017 "Organisation of the Ministry of Finance", P.D. 85/2005 "Organization of the Special Audit Service (S.A.S.) of the Ministry of Economy and Finance", Law No. 3296/2004, Law No. 4336/2015.

²⁹⁷ Law No. 4336/2015 (article 2 par. D subparagraph D7)

²⁹⁸ L. 4389/2016

²⁹⁹ Articles 66 et seq. of the Tax Procedure Code (TPC, Law No. 4174/93, A170).

³⁰⁰ They are located in Athens and Thessaloniki with territorial jurisdiction as defined by Law No. 4249/2014.

³⁰¹ L. 4249/2014 article 24 and Annual Report of the Economic Police Directorate 2016

investigation department for money laundering and is therefore also staffed by specialised personnel³⁰². With regard to money laundering cases, the Department of Economic Protection is de facto competent.

Cyber Crime Division (CCD), which is responsible for the prevention, investigation and repression of crimes committed through the Internet. Specifically, the Department of Special Affairs and Prosecution of Electronic Economic Crimes has the competence to fight economic crimes committed in an online environment.

Directorate for Internal Affairs (DIA), responsible for³⁰³ tackling the phenomenon of corruption, investigating and prosecuting crimes under Law 2713/1999 committed or assisted by police officers, officials or civil servants of the wider public sector, employees and officials of the European Union or international organisations operating in the Greek territory.

Organised Crime and Human Trafficking Sub-Division (OCHTSD) at the Police Directorate of Attica and Thessaloniki (one per Directorate) with the task of preventing and repressing extremely serious criminal offences related to public and state security and in particular offences that have the characteristics of organised crime, conducting investigations to detect illegal proceeds³⁰⁴.

Department for the Protection of Property Rights (DPPR) at the Attica and Thessaloniki Police Directorate (one per Directorate) dealing mainly with cases of fraud and forgery, by examining tax and banking data on a prosecutor's order³⁰⁵.

³⁰² Specialised Officers with Financial, Banking, Taxation and Accounting specialisations, holders of postgraduate qualifications and with related work experience in the private sector (banks, auditing companies, etc.).

³⁰³ L. 2713/1999

³⁰⁴ P.D. 7/2017 article 2

³⁰⁵ L. 3691/2008, art. 50

IV TYPES OF LEGAL DOCUMENTS

S/N	LEGAL DOCUMENT	ISSUING AUTHORITY	INFORMATION PROVIDED FOR CONFIRMING IDENTITY	ELIGIBLE HOLDERS	APPEARANCE/ CONTENT OF DOCUMENT
MINISTRY OF CITIZEN PROTECTION					
1	POLICE IDENTITY CARD	HELLENIC POLICE HEADQUARTERS - SECURITY DEPARTMENTS	PHOTOGRAPH, SURNAME, NAME, FATHER'S NAME-MOTHER'S NAME, DATE OF BIRTH	HOLDERS OF GREEK CITIZENSHIP	NUMBERED-LAMINATED-PHOTOGRAPH-NATIONAL SEAL
2	PASSPORT	HELLENIC POLICE HEADQUARTERS - PASSPORT ISSUING DIRECTORATE	PHOTOGRAPH, SURNAME, NAME, FATHER'S NAME, DATE OF BIRTH, PLACE OF BIRTH, NATIONALITY	HOLDERS OF GREEK CITIZENSHIP	PASSPORT OF THE HELLENIC REPUBLIC
3	POLICE PERSONNEL IDENTITY CARD	HELLENIC POLICE HEADQUARTERS	PHOTOGRAPH, SURNAME, NAME, FATHER'S NAME, MOTHER'S NAME, DATE OF BIRTH, PLACE OF BIRTH	HELLENIC POLICE PERSONNEL	PLASTIC CARD. HAS A UNIQUE SERIAL NUMBER ON THE REVERSE SIDE
4	CERTIFICATION OF IDENTITY	HELLENIC POLICE HEADQUARTERS	PHOTOGRAPH, SURNAME, NAME, FATHER'S NAME, MOTHER'S NAME, DATE OF BIRTH	CERTIFIES THAT THE PERSON NAMED BELOW WITH GENERAL REGISTRY NUMBER HAS YET TO BE ISSUED A SERVICE IDENTITY CARD ON RETURN TO ACTIVE DUTY-THIS CERTIFICATE IS ISSUED AS TEMPORARY CERTIFICATION OF HIS/HER IDENTITY	A4-NATIONAL SEAL, ROUND STAMP, COMMISSIONER'S SIGNATURE
5	SINGLE RESIDENCE PERMIT	ASYLUM DEPARTMENT OF THE MINISTRY OF MIGRATION POLICY	PHOTOGRAPH, SURNAME, NAME, DATE OF BIRTH, WITHOUT FATHER'S NAME-MOTHER'S NAME	a) CATEGORY ELIGIBLE FOR INTERNATIONAL PROTECTION (REFUGEE) b) PERSON OF GREEK ORIGIN	a) GRC INDICATION-NUMBERED-LAMINATED-PHOTOGRAPH-NATIONAL SEAL-SECURITY CHARACTERISTICS
6	ALIEN'S RESIDENCE PERMIT	MINISTRY OF INTERIOR-CITIZEN PROTECTION DIVISION, ATTICA ALIENS DIRECTORATE or ALIENS OFFICE or POLITICAL ASYLUM DEPARTMENT	PHOTOGRAPH, SURNAME, NAME, FATHER'S NAME-DATE OF BIRTH-RESIDENTIAL ADDRESS	CATEGORIES: a) WITH SUBSIDIARY PROTECTION STAMP b) AND ELIGIBLE FOR RESIDENCY STATUS FOR HUMANITARIAN REASONS (OF KURDISH ORIGIN) c) POLITICAL ASYLUM DEPARTMENT-POLITICAL REFUGEE GRATIS (AFGHANISTAN)	BIFOLD - ROUND STAMP
7	INTERNATIONAL PROTECTION APPLICANT'S	ASYLUM DEPARTMENT OF THE MINISTRY OF MIGRATION POLICY	PHOTOGRAPH, SURNAME, NAME, FATHER'S NAME,	CONTAINS DATE OF SUBMISSION OF APPLICATION, DATE OF	TRIFOLD WITH PHOTOGRAPH

	CARD		MOTHER'S NAME, DATE OF BIRTH, RESIDENTIAL ADDRESS	EXAMINATION OF APPEAL & EXPIRATION DATE	
8	ALIEN APPLICANT FOR ASYLUM ID CARD	MINISTRY OF INTERIOR-CITIZEN PROTECTION DIVISION-HELLENIC POLICE HEADQUARTERS	PHOTOGRAPH, SURNAME, NAME, FATHER'S NAME, MOTHER'S NAME, DATE OF BIRTH, RESIDENTIAL ADDRESS		TRIFOLD - ROUND STAMP
9	SPECIAL ID CARD FOR ALIEN WHO HAS REQUESTED RECOGNITION AS A REFUGEE	MINISTRY OF PUBLIC ORDER-PREFECTURE SECURITY SUBDIRECTORATE	PHOTOGRAPH, SURNAME, NAME, FATHER'S NAME, MOTHER'S NAME, DATE OF BIRTH, RESIDENTIAL ADDRESS		TRIFOLD- TEMPLATE KA- 144
10	OFFICIAL MEMO	POLICE DEPARTMENTS	PHOTOGRAPH, SURNAME, NAME, FATHER'S NAME, MOTHER'S NAME, DATE OF BIRTH	THE ALIEN WITH THE IDENTITY INFORMATION BELOW WAS ISSUED WITH A CERTIFICATE OF INABILITY TO DEPART NO.	A4 - MEMO ISSUED TO AN ALIEN WHO IS RELEASED FROM HOLDING
11	MEMO	ALIENS DIRECTORATE/OFFICE OF ADMINISTRATIVE MEASURES	PHOTOGRAPH, SURNAME, NAME, FATHER'S NAME, MOTHER'S NAME, DATE OF BIRTH	Police officer of the Asylum Service/Political Asylum Department issued to the alien citizen of Decision no. ... of the 1st Refugees Committee by which his/her appeal was NOT accepted and the capacity of refugee was NOT recognized in his/her person The present document is issued gratis and must be surrendered to the Passport Control Service on exiting the country.	A4, POLICE LOGO, ROUND STAMP
12	PROOF OF SERVICE OF NOTIFICATION	4TH REFUGEES COMMITTEE OF THE MINISTRY OF INTERIOR-CITIZEN PROTECTION DIVISION	NO (ALTHOUGH COMPLETE INFORMATION EXISTS)	DOCUMENT SERVED IN CASE OF REJECTION OF APPEAL (VIA SERVICE PROCEDURE)	AS A SERVED DOCUMENT- WITHOUT PHOTOGRAPH
13	CERTIFICATE OF SUBMISSION OF APPLICATION FOR ISSUING OF RESIDENCE PERMIT	ALIENS DEPARTMENT	PHOTOGRAPH, SURNAME, NAME, FATHER'S NAME, FIELD FOR PASSPORT NO. (NOT ALWAYS FILLED OUT)-WITHOUT DATE OF BIRTH	TEN-YEAR RESIDENCE PERMIT (LAW3731/08 article 39, paragraph 1)- (RENEWAL) (Also written, in cases of renewal: "The relevant application was submitted in a timely manner and with complete documentation and the present certificate is valid temporarily, until the relevant decision is issued") EXCEPTIONAL REASONS- EMPLOYMENT AND PROVISION OF	A4-COLOURED- NATIONAL SEAL-ROUND STAMP

				SERVICES OR PROJECT 1010 (FIRST INSTANCE)	
				RESIDENCY PERMIT FOR EMPLOYMENT AND PROVISION OF SERVICES OR PROJECT (RENEWAL)	
				FAMILY MEMBERS OF A GREEK CITIZEN-EMPLOYMENT, PROVISION OF SERVICES OR PROJECT AND PROFESSIONAL ACTIVITIES (FIRST INSTANCE)	
				FAMILY MEMBERS OF THIRD-COUNTRY CITIZEN (PRESIDENTIAL DECREEE 131/06) (RENEWAL)	
				EMPLOYMENT, LAW 3083/05, article.15, paragraph.1 (RENEWAL)	
14	SPECIAL CERTIFICATE OF LEGAL RESIDENCY	HELLENIC POLICE-REGIONAL ALIENS DEPARTMENT	PHOTOGRAPH, SURNAME, NAME, FATHER'S NAME, MOTHER'S NAME, DATE OF BIRTH, FIELD FOR PASSPORT NO. (WHEN THERE IS ONE)	"Certifies that the holder of this document has a temporary right to reside and work in Greece, based on article 1 of Ministerial Decision 4000/3/84 of 15/01/2014." -	A4 PAPER WITH PHOTOGRAPH
15	CERTIFICATION OF SUBMISSION OF DOCUMENTATION FOR THE ISSUING OF A SINGLE RESIDENCE PERMIT AND SPECIAL IDENTITY CARD FOR ALIENS OF GREEK DESCENT	MINISTRY OF INTERIOR-CITIZEN PROTECTION DIVISION	PHOTOGRAPH-FATHER'S NAME-DATE OF BIRTH-PASSPORT NO.	CONSTITUTES PROOF OF LEGAL RESIDENCY AND WORK IN OUR COUNTRY. POSSESSION DOES NOT PREJUDICE THE DECISION ON APPROVAL OR REJECTION OF APPLICATION	A4 PAPER WITH PHOTOGRAPH
16	TRAVEL DOCUMENT CONVENTION OF 28 JULY 1951	ALIENS DIRECTORATES	PHOTOGRAPH, SURNAME, NAME, DATE OF BIRTH, WITHOUT FATHER'S NAME-MOTHER'S NAME	THIS DOCUMENT IS VALID FOR ALL COUNTRIES EXCEPT ...	BLUE COLOUR - ALSO CONTAINS PASSPORT NO.
17	CERTIFICATE OF REGISTRATION OF A CITIZEN OF A MEMBER STATE OF THE EUROPEAN UNION	REGIONAL ALIENS DEPARTMENT (HELLENIC POLICE) OF THE MINISTRY OF INTERIOR-CITIZEN PROTECTION DIVISION	PHOTOGRAPH, SURNAME, NAME, DATE OF BIRTH, RESIDENTIAL ADDRESS, WITHOUT FATHER'S NAME-MOTHER'S NAME-DATE OF BIRTH	THE PRESENT DOCUMENT, WHICH IS ISSUED IN ACCORDANCE WITH THE PROVISIONS OF PRESIDENTIAL DECREE 106/2007, CERTIFIES THAT THE AFOREMENTIONED CITIZEN (e.g. OF GERMANY) REGISTERED HIS RESIDENCY IN GREECE FOR ... MEMBER OF EU FAMILY	BIFOLD, ROUND STAMP

18	DOCUMENT CERTIFYING PERMANENT RESIDENCY OF A CITIZEN OF A MEMBER STATE OF THE EUROPEAN UNION	REGIONAL ALIENS DEPARTMENT (HELLENIC POLICE) OF THE MINISTRY OF INTERIOR-CITIZEN PROTECTION DIVISION	PHOTOGRAPH, SURNAME, NAME, RESIDENTIAL ADDRESS, WITHOUT FATHER'S NAME-MOTHER'S NAME-DATE OF BIRTH	WITH THE PRESENT DOCUMENT, WHICH IS ISSUED IN ACCORDANCE WITH THE PROVISIONS OF PRESIDENTIAL DECREE 106/2007, THE ABOVE CITIZEN (e.g. OF SPAIN) RESIDES PERMANENTLY IN GREECE.	BIFOLD, ROUND STAMP
----	---	--	---	--	---------------------

Ministry of Migration Policy

19	INTERNATIONAL PROTECTION APPLICANT'S CARD	ASYLUM SERVICE	PHOTOGRAPH, SURNAME, NAME, FATHER'S NAME, MOTHER'S NAME, DATE OF BIRTH, RESIDENTIAL ADDRESS	CONTAINS DATE OF INTERVIEW OR DATE OF EXAMINATION OF APPEAL & EXPIRATION DATE	TRIFOLD WITH PHOTOGRAPH
20	INTERNATIONAL PROTECTION APPLICANT'S CARD (FULL REGISTRATION)		PHOTOGRAPH, SURNAME, NAME, FATHER'S NAME, MOTHER'S NAME, DATE OF BIRTH, RESIDENTIAL ADDRESS	CONTAINS DATE OF INTERVIEW OR DATE OF EXAMINATION OF APPEAL & EXPIRATION DATE	TRIFOLD WITH PHOTOGRAPH
21	INTERNATIONAL PROTECTION APPLICANT'S CARD (TEMPORARY REGISTRATION VIA SKYPE)		PHOTOGRAPH, SURNAME, NAME, FATHER'S NAME, MOTHER'S NAME, DATE OF BIRTH, RESIDENTIAL ADDRESS	STATES DATE OF REGISTRATION, ASYLUM OFFICE & EXPIRATION DATE	TRIFOLD WITH PHOTOGRAPH
22	TRAVEL DOCUMENT FOR PERSONS ELIGIBLE FOR SUBSIDIARY PROTECTION		PHOTOGRAPH, SURNAME, NAME, DATE OF BIRTH, PLACE OF BIRTH, NATIONALITY	ALIEN'S TRAVEL DOCUMENT	GREEN PASSPORT OF THE HELLENIC REPUBLIC
23	TRAVEL DOCUMENT FOR PERSONS ELIGIBLE FOR REFUGEE STATUS		PHOTOGRAPH, SURNAME, NAME, DATE OF BIRTH, PLACE OF BIRTH, NATIONALITY	TRAVEL DOCUMENT CONVENTION OF 28 JULY 1951	BLUE PASSPORT OF THE HELLENIC REPUBLIC
24	RESIDENCE PERMIT		PHOTOGRAPH, SURNAME, NAME, DATE OF BIRTH, PLACE OF BIRTH, CITIZENSHIP	PERSON ELIGIBLE FOR INTERNATIONAL PROTECTION AS A REFUGEE	PLASTIC CARD. HAS A UNIQUE SERIAL NUMBER ON THE REVERSE SIDE

MINISTRY OF INTERIOR

25	PERMANENT RESIDENCY CARD FOR FAMILY MEMBERS OF AN EU CITIZEN	MINISTRY OF INTERIOR, PUBLIC ADMINISTRATION & DECENTRALIZATION, ATTICA REGION	PHOTOGRAPH, SURNAME, NAME, DATE OF BIRTH, WITHOUT FATHER'S NAME-MOTHER'S NAME	GRANTS RIGHT OF ACCESS TO THE LABOUR MARKET	SIZE OF IDENTITY CARD, LAMINATED, ROUND STAMP
26	DECISION	THE SECRETARY GENERAL FOR ATTICA DECENTRALIZED ADMINISTRATION (DIRECTORATE GENERAL FOR INTERNAL OPERATION, DIRECTORATE FOR	PHOTOGRAPH, SURNAME, NAME, FATHER'S NAME, DATE OF BIRTH	WE DECIDE: WE RENEW A TEN-YEAR RESIDENCE PERMIT FOR THE (e.g. TURKISH) CITIZEN ..., DEPRIVED OF PASSPORT	A4-NATIONAL SEAL-ROUND STAMP

		ALIENS AND MIGRATION			
27	PROOF OF RECEIPT OF APPLICATION	MINISTRY OF INTERIOR- SECRETARIAT GENERAL FOR POPULATION AND SOCIAL COHESION	SURNAME, NAME, FATHER'S NAME, PASSPORT NO., WITHOUT PHOTOGRAPH	Mr/Ms ... holder of passport no. submitted to our service an application for GRANTING/EXCEPTION AL REASONS (LAW4251/14) with reference no. On The above proof of receipt is not proof of legal residency in the country.” -	A4-NATIONAL SEAL-ROUND STAMP
28	CERTIFICATE OF SUBMISSION OF APPLICATION FOR ISSUING OF RESIDENCE PERMIT	MINISTRY OF INTERIOR-ALIENS AND MIGRATION DIRECTORATE	PHOTOGRAPH, SURNAME, NAME, FATHER'S NAME, FIELD FOR PASSPORT NO. (NOT ALWAYS FILLED OUT)-WITHOUT DATE OF BIRTH	TEN-YEAR RESIDENCE PERMIT (LAW3731/08 article 39, paragraph 1)- (RENEWAL) (Also written, in cases of renewal: “The relevant application was submitted in a timely manner and with complete documentation and the present certificate is valid temporarily, until the relevant decision is issued”	A4-COLOURED- NATIONAL SEAL-ROUND STAMP
29				HUMANITARIAN REASONS-ADULTS BORN IN GREECE (LAW3386/05 article 44, paragraph 1) (FIRST INSTANCE)	
30	CERTIFICATE OF SUBMISSION OF APPLICATION FOR ISSUING OF RESIDENCE PERMIT	MINISTRY OF INTERIOR-ALIENS AND MIGRATION DIRECTORATE OR MUNICIPALITY	PHOTOGRAPH, SURNAME, NAME, FATHER'S NAME, MOTHER'S NAME, DATE OF BIRTH	RESIDENCE PERMIT FOR HUMANITARIAN REASONS, EMPLOYMENT 1000- RENEWAL OR TEN- YEAR RESIDENCE PERMIT (LAW 3731/2008 ARTICLE 9, PARAGRAPH 1-RENEWAL) OR HUMANITARIAN REASONS-ADULTS WHO ATTENDED GREEK SCHOOLS (LAW 3386/05 ARTICLE 44, PARAGRAPH 1viii- RENEWAL)	A4-ROUND STAMP
MINISTRY OF NATIONAL DEFENSE					
31	MILITARY IDENTITY CARD	ARMY GENERAL STAFF-NAVY GENERAL STAFF-AIRFORCE GENERAL STAFF	PHOTOGRAPH, SURNAME, NAME, FATHER'S NAME, MOTHER'S NAME, DATE OF BIRTH	PERMANENT MILITARY PERSONNEL AND RESERVISTS	SIZE OF IDENTITY CARD, LAMINATED, ROUND STAMP
MINISTRY OF SHIPPING AND ISLAND POLICY					
32	COAST GUARD PERSONNEL IDENTITY CARD	COAST GUARD HEADQUARTERS	PHOTOGRAPH, SURNAME, NAME, FATHER'S NAME, MOTHER'S NAME, DATE OF BIRTH, PLACE OF BIRTH	COAST GUARD PERSONNEL	PLASTIC CARD. HAS A UNIQUE SERIAL NUMBER ON THE REVERSE SIDE

V CAPITAL MARKET SECTOR

LEGAL FRAMEWORK

Laws

- L. 3691/2008 (Government Gazette, Series I, No 166/5-8-2008) 'Prevention and suppression of money laundering and terrorist financing and other provisions'

The Rules of the Hellenic Capital Market Commission

- 1/506/8.4.2009 "preventing the use of the financial system for money laundering and terrorist financing"
- 34/586/26.5.2011 (Government Gazette B' 1428/16.6.2011) 'Apply human rights due diligence in cases of outsourcing or agency'
- 35/586/26.5.2011 (Government Gazette B' 1428/16.6.2011) Amending Decision 1/506/8.4.2009 (Government Gazette B/834/6.5.2009) of the Board of Directors of the Capital Market Commission 'preventing the use of the financial system for money laundering and terrorist financing'

Circulars Hellenic Capital Market Commission

- No 52 'Clarifications on the information of the Annual Report of par 10. 2 of Decision 1/506/2009 of the Capital Market Commission regarding the prevention and suppression of money laundering and terrorist financing'
- No 49 "Identify and report to the competent authority under Article. 7 of Law 3691/2008, transactions suspicion of committing fraud and/or legalization of property derived by this transaction, and Typology of suspicious and unusual transactions related to the basic offense of tax evasion (Article par 77. 1 of law 3842/2010)'
- No 41 "Indicative Typology of suspicious transactions/money laundering activities from criminal activities and terrorist financing."