

FATF



Anti-money laundering and counter-terrorist financing measures

Finland

Mutual Evaluation Report

April 2019





The Financial Action Task Force (FATF) is an independent inter-governmental body that develops and promotes policies to protect the global financial system against money laundering, terrorist financing and the financing of proliferation of weapons of mass destruction. The FATF Recommendations are recognised as the global anti-money laundering (AML) and counter-terrorist financing (CTF) standard.

For more information about the FATF, please visit the website: www.fatf-gafi.org.

This document and/or any map included herein are without prejudice to the status of or sovereignty over any territory, to the delimitation of international frontiers and boundaries and to the name of any territory, city or area.

This assessment was adopted by the FATF at its February 2019 Plenary meeting.

Citing reference:

FATF (2019), *Anti-money laundering and counter-terrorist financing measures – Finland*,
Fourth Round Mutual Evaluation Report, FATF, Paris
<http://www.fatf-gafi.org/publications/mutualevaluations/documents/mer-finland-2019.html>

© 2019 FATF-. All rights reserved.

No reproduction or translation of this publication may be made without prior written permission.

Applications for such permission, for all or part of this publication, should be made to

the FATF Secretariat, 2 rue André Pascal 75775 Paris Cedex 16, France

(fax: +33 1 44 30 61 37 or e-mail: contact@fatf-gafi.org).

Photo Credit - Cover: © Ministry of Interior Public Relations, Finland

Table of contents

Key Findings.....	5
Risks and General Situation.....	6
Overall Level of Compliance and Effectiveness.....	7
Priority Actions.....	13
Effectiveness & Technical Compliance Ratings.....	14
MUTUAL EVALUATION REPORT.....	15
Preface	15
CHAPTER 1. ML/TF RISKS AND CONTEXT.....	17
ML/TF Risks and Scoping of Higher Risk Issues.....	18
Materiality.....	21
Structural Elements.....	22
Background and Other Contextual Factors.....	22
CHAPTER 2.NATIONAL AML/CFT POLICIES AND CO-ORDINATION	37
Key Findings and Recommended Actions.....	37
Immediate Outcome 1 (Risk, Policy and Co-ordination)	38
CHAPTER 3. LEGAL SYSTEM AND OPERATIONAL ISSUES	47
Key Findings and Recommended Actions.....	47
Immediate Outcome 6 (Financial Intelligence ML/TF).....	50
Immediate Outcome 7 (ML investigation and prosecution).....	61
Immediate Outcome 8 (Confiscation).....	72
CHAPTER 4. TERRORIST FINANCING AND FINANCING OF PROLIFERATION	81
Key Findings and Recommended Actions.....	81
Immediate Outcome 9 (TF investigation and prosecution)	84
Immediate Outcome 10 (TF preventive measures and financial sanctions)	93
Immediate Outcome 11 (PF financial sanctions).....	97
CHAPTER 5. PREVENTIVE MEASURES	103
Key Findings and Recommended Actions.....	103
Immediate Outcome 4 (Preventive Measures).....	104
CHAPTER 6. SUPERVISION	115
Key Findings and Recommended Actions.....	115
Immediate Outcome 3 (Supervision).....	117
CHAPTER 7. LEGAL PERSONS AND ARRANGEMENTS	133
Key Findings and Recommended Actions.....	133
Immediate Outcome 5 (Legal Persons and Arrangements)	134

CHAPTER 8. INTERNATIONAL CO-OPERATION.....	141
Key Findings and Recommended Actions.....	141
Immediate Outcome 2 (International Co-operation).....	142
Technical Compliance Annex.....	151
Recommendation 1 – Assessing risks and applying a risk-based approach	151
Recommendation 2 – National cooperation and coordination.....	153
Recommendation 3 – Money Laundering Offence.....	154
Recommendation 4 – Confiscation and Provisional Measures.....	157
Recommendation 5 – Terrorist Financing Offence.....	159
Recommendation 6 – Targeted Financial Sanctions related to Terrorism and Terrorist Financing	161
Recommendation 7 – Targeted Financial Sanctions related to Proliferation.....	167
Recommendation 8 – Non-Profit Organisations (NPOs).....	170
Recommendation 9 - Financial institution secrecy laws.....	174
Recommendation 10 – Customer Due Diligence.....	176
Recommendation 11 – Record keeping	178
Recommendation 12 – Politically Exposed Persons (PEPs).....	179
Recommendation 13 – Correspondent Banking	180
Recommendation 14 - Money or Value Transfer Services (MVTs)	180
Recommendation 15 - New Technologies.....	181
Recommendation 16 – Wire Transfers	182
Recommendation 17 - Reliance on Third Parties	184
Recommendation 18 – Internal controls and foreign branches and subsidiaries	185
Recommendation 19 - Higher Risk Countries	186
Recommendation 20 – Reporting of Suspicious Transactions	186
Recommendation 21 – Tipping-off and confidentiality.....	186
Recommendation 22 – Designated Non-Financial Businesses And Professions (DNFBPs): Customer Due Diligence.....	187
Recommendation 23 - Designated Non-Financial Businesses And Professions (DNFBPs): Other measures.....	189
Recommendation 24 – Transparency and beneficial ownership of legal persons	190
Recommendation 25 - Transparency and beneficial ownership of legal arrangements.....	196
Recommendation 26 – Regulation and supervision of financial institutions.....	197
Recommendation 27 – Powers of supervisors	202
Recommendation 28 – Regulation and supervision of DNFBPs	204
Recommendation 29 – Financial Intelligence Units (FIU).....	207
Recommendation 30 – Responsibilities of Law Enforcement and Investigative Authorities.....	210
Recommendation 31 – Powers of Law Enforcement and Investigative Authorities	211
Recommendation 32 – Cash Couriers.....	213
Recommendation 33 – Statistics.....	215
Recommendation 34 – Guidance and feedback.....	216
Recommendation 35 – Sanctions.....	217
Recommendation 36 – International instruments	218
Recommendation 37 – Mutual legal assistance (MLA).....	219
Recommendation 38 – Mutual legal assistance (MLA): freezing and confiscation	221
Recommendation 39 – Extradition	223
Recommendation 40 – Other forms of international cooperation.....	224
Summary of Technical Compliance – Key Deficiencies.....	230
Glossary of Acronyms	235

Executive Summary

1. This report summarises the AML/CFT measures in place in Finland as at the date of the on-site visit (23 May to 8 June 2018). It analyses the level of compliance with the FATF 40 Recommendations and the level of effectiveness of Finland's AML/CFT system, and provides recommendations on how the system could be strengthened.

Key Findings

- a) Finland has an adequate level of understanding of its Money Laundering (ML) and Terrorist Financing (TF) risks, and especially of its main ML risks associated to the grey economy. Those risks are addressed in a well-coordinated manner and through an efficient and comprehensive set of preventive measures. Key national authorities for combating TF have a sound understanding of TF risks. They address the identified TF risks in a manner which is consistent with the nature and level of TF risk in the country.
- b) Financial intelligence is used to a high extent to develop evidence and trace criminal proceeds. FIU conducts quality analysis but its products are not used to a full extent by other authorities.
- c) Authorities conduct complex and international ML investigations involving foreign predicate offences and significant amounts of laundered proceeds. ML investigations and prosecutions are consistent with the country's risk profile, with priority given to grey economy-related offending and economic crimes. However, some technical limitations impact Finland's effectiveness regarding ML investigations and prosecutions, in particular the rule of concurrent offences and the sanction regime.
- d) Although TF prosecutions have been initiated, there has been no conviction to date in Finland. This is broadly in line with the overall TF risks in the country even though the changing environment, with increased focus on ISIL Foreign Terrorists Fighters (FTFs) and returnees, are not adequately reflected in TF cases investigated. National authorities are mobilised on the terrorism threat, and intelligence on TF shared between the Financial Intelligence Unit (FIU) and the security intelligence service (SUPO) results in TF leads. Targeted Financial Sanctions (TFS) are used only to some extent as mitigation measures, in particular with regard to FTFs. There is limited interaction to date with the Non-Profit Organisation (NPO) sector at risk of TF.

- e) Finland has developed a far-reaching legal system to recover assets, including mechanisms to facilitate decisions to confiscate. Cases evidence that freezing and seizure measures are routinely used by the relevant authorities. However, Finnish authorities do not demonstrate whether the policies are actually successful in permanently depriving criminals of their assets. In any case, confiscations in cross-border ML cases and repatriation of assets to Finland are insignificant, and confiscation in cross-border cash transportation cases is not applied to a satisfactory extent.
- f) Financial Institutions (FIs) have an adequate understanding of their exposure to ML risks and of their AML/CFT obligations. However, there are some gaps on the TF side, and some high-risk institutions such as hawalas need to improve their ML/TF knowledge. The level of understanding of risk and awareness of AML/CFT obligations of Designated Non-Financial Businesses and Professions (DNFBPs) is adequate only in some sectors. STR reporting is low to non-existent for some DNFBP sectors.
- g) Supervisors' understanding of ML/TF risks is not adequate for the majority of sectors under their supervision, and overall, the AML/CFT monitoring and supervision is not carried out on a risk-sensitive basis. The supervisors are significantly under-resourced given the breadth and depth of their AML/CFT responsibilities and associated workload.
- h) The ability of competent authorities to establish the beneficiary ownership (BO) of legal persons in a timely manner is limited. The public registries are not fully reliable and relevant remedies to ensure that registers are kept up-to-date are not available.
- i) Finnish authorities cooperate routinely with their foreign counterparts, formally and informally. Law Enforcement Authorities (LEAs) in particular both seek international cooperation to build their cases, and share timely and accurate information. Cooperation is generally in line with Finland's geographic risk exposure.
- j) There is a satisfactory level of coordination and cooperation in relation to combating Proliferation Financing (PF) matters in Finland. Mechanisms for the implementation of TFS are in place, with European Union (EU) delays for transposition mitigated by prior designations by the EU for Iran.

Risks and General Situation

2. The main risk of financial crime in Finland stems from the grey economy. The main ML threat in that connection is the proceeds resulting from non-payment of statutory payments and taxes, as well as tax fraud. Proceeds generated from both domestic and foreign frauds and proceeds from drug crimes are the other highest ML risks in the country. A significant part of the proceeds of crimes generated in Finland is moved outside of the country. Main ML methods are the use of front companies, complex corporate structures and front persons, cash couriers and wire transfers.

3. Main TF risks stem from sympathisers of terrorist cause and FTFs, with a strong focus on ISIL FTFs and returnees. Main methods are money transfers, including through registered and unregistered hawalas, and misuse of NPOs.

4. A factor that contributes to limiting the ML/TF risk is the relatively low use of cash. Given its geographical location, Finland is a major European gateway to and from non-European countries, and strong business and trade relationships have developed between Finland and Russia, as well as with neighbouring Baltic States and other Nordic countries. This geographic proximity supports the development of commercial routes, including trade routes in illicit flows of goods and funds.

Overall Level of Compliance and Effectiveness

5. Finland has brought a number of technical changes to its AML/CFT preventive regime, with the AML/CFT Act which entered into force in 2017. For instance, it introduced obligations regarding the development of risk assessments by FIs and DNFBPs and the application of risk-based mitigation measures. It also broadened the scope of application of beneficial ownership requirements and strengthened obliged entities' internal control requirements. However, significant shortcomings are still noted, in particular for the transparency regime applicable to legal persons, the supervisory measures applicable to DNFBPs, and the sanction regime for failure to comply with the preventive measures in general. In addition, there are still technical deficiencies affecting in particular the TF offence and the regime applicable to NPOs at risk of TF abuse.

6. Finland is highly effective regarding international cooperation. It achieves a substantial level of effectiveness in the assessment of ML/TF risks and domestic coordination, as well as in the collection and use of financial intelligence and other information and in ML investigations and prosecution. Finland demonstrates a moderate level of effectiveness in areas related to TF investigations, prosecutions and preventive measures and the use of Targeted Financial Sanctions (TFS) for countering TF and PF, as well as on the implementation of preventive measures by FIs and DNFBPs, the prevention of misuse of legal persons and arrangements, and the confiscation of criminals' proceeds of crime or property of equivalent value. Finland achieves a low level of effectiveness regarding supervision of FIs and DNFBPs. Generally speaking, Finland needs to enhance its collection and maintenance of comprehensive ML/TF-related statistics in order to better document its analysis of ML/TF risks, as well as to demonstrate the actions it has taken and the results achieved.

Assessment of risk, coordination and policy setting (Chapter 2; IO.1, R.1, 2, 33 & 34)

7. Finland has an adequate understanding of its ML/TF risks and in particular of its main ML risks, associated with the grey economy. The National Strategy on the Prevention of the Grey Economy and Economic Crime sets a relevant framework to address the main identified ML risks in a coordinated manner and puts forward an efficient preventive approach to economic crime. Other major ML risks identified in Finland - frauds and drugs - are generally adequately addressed by Finnish authorities, based on mutually supportive actions between relevant authorities. There are concerns regarding supervisors' overall understanding of ML risks.

8. Key national authorities for combating TF have a sound understanding of TF risks. They address the identified TF risks in a manner which is consistent with the nature and level of TF risk in the country.
9. To further improve the understanding of the ML/TF risks and to ensure that there is a shared and continuous understanding by all relevant authorities, Finland should update the National Risk Assessment (NRA) conducted in 2014/15 and adopt an Action Plan alongside, including the resources required to successfully and efficiently conduct the planned activities.
10. The AML/CFT priorities and activities of the law enforcement community, intelligence and Tax authorities are aligned with the national risk picture. However, supervisors' ML/TF risk-driven objectives and activities are limited.
11. Co-operation and co-ordination between LEAs, FIU, Tax authorities and SUPO is adequate, but the level of cooperation and coordination between AML/CFT supervisors, and between supervisors and the FIU is not sufficient. The recently established AML/CFT Coordination Group should be operationalized shortly to help improve the dialogue and interaction between those authorities.
12. There is a satisfactory level of coordination and cooperation in relation to CPF matters.

Financial intelligence, ML investigations, prosecutions and confiscation (Chapter 3; IO.6, 7, 8; R.1, 3, 4, 29–32)

13. Financial intelligence along with other relevant information is used to a high extent in investigations to develop evidence and trace criminal proceeds related to ML and associated predicate offences. Financial intelligence plays an important role in Countering the Financing of Terrorism (CFT) domain as well. However, Finland should encourage LEAs (especially local police departments) to engage more actively with the FIU to leverage its potential.
14. There is a wide range of different reports available to competent authorities, including the “compliance reports” produced by the Tax Administration, with most of them containing accurate and relevant information. The authorities actively request and receive these reports in order to perform their duties.
15. The FIU’s analysis and dissemination supports the operational needs of the competent authorities to a moderate extent. The FIU products contribute both to starting new criminal investigations and to supporting the ongoing cases. However, the overall number of ML cases using intelligence products of the FIU is modest. The FIU produces quality strategic analysis, but Finland should urge competent authorities, especially supervisors, to make more active use of it.
16. Finland’s ML investigations, prosecutions and convictions seem in line with its ML threats and risks in terms of number of investigations, prosecutions and convictions. Authorities do conduct complex investigations involving foreign predicate offences and significant amounts of laundered proceeds, with priority given to grey economy-related offending and economic crimes, consistently with the country’s risk profile. The focus is also on fraud and narcotics-related offences (with a focus on individual dealers rather than on organised crime groups), and third-party ML. Cases are brought to courts by the prosecution service to a satisfactory extent.

17. Penalties for ML offences are not fully proportional, as cumulative fines and unconditional imprisonment are not possible. Courts do not use the full range of penalties available and sentencing practice is lenient.

18. Finland has developed a far-reaching legal system to recover assets, including provisional measures and mechanisms to facilitate decisions to confiscate. Cases evidence that freezing and seizures measures are routinely used by the relevant authorities.

19. Seized amounts are compensated to the victims as a matter of priority in Finland, over confiscation to the State. Therefore the confiscation decisions, and the amounts involved, do not fully reflect the extent to which criminals are deprived of their assets. Nevertheless, Finnish authorities, despite their high-level engagement, lack comprehensive statistics to demonstrate and assess whether the policies are actually successful in permanently depriving criminals of their assets. In any case, confiscations in cross-border ML cases and repatriation of assets to Finland are insignificant, and confiscation in cross-border cash transportation cases is not applied to a satisfactory extent.

20. As regards deprivation of assets related to TF, it is not fully in line with the country's risk profile as only limited steps have been taken to freeze assets of FTFs.

Terrorist and proliferation financing (Chapter 4; IO.9, 10, 11; R. 1, 4, 5–8, 30, 31 & 39.)

21. TF cases are well identified, usually based on information from the FIU and SUPO. The quality of investigations is generally high and based on a collaborative approach between relevant authorities. LEAs, with SUPO's input, are able to mobilise joint investigative teams with international counterparts and use advanced investigative tools.

22. TF is part of every terrorism related investigation, but is not usually pursued as a distinct criminal activity. TF prosecutions have been initiated, but there have been no convictions to date. This is broadly in line with the overall TF risk in Finland. However, the changes in the TF environment - with a strong focus on ISIL FTFs and returnees - are not reflected in TF cases, as there has been no investigation of FTF and returnees so far. Finnish authorities need to increase their focus on these specific risks, as well as get the required skilled and dedicated human resources to deal with the increasing mobilisation on TF risks.

23. The TF offence legal framework does not criminalise the financing of an individual terrorist without a link to the use of funds to finance a specific offence. Clarification of the applicable legislation is required on this point.

24. Finland has measures in place to implement TFS for TF. However, implementation is not without delay nor fully effective, mainly because of technical deficiencies inherent to applicable European Union (EU) regulations. TFS are used only to some extent as mitigation measures, in particular with regard to FTFs. Finland has successfully frozen terrorist related assets but to a very limited extent.

25. Finland has identified NPOs receiving state subsidies, NPOs active in conflict zones and immigrant based NPOs as the subset of NPOs at risk of TF abuse. However, its analysis is not up-to-date. Finland still needs to provide guidance, conduct outreach activity and develop focused actions vis-à-vis potentially vulnerable NPOs to prevent their possible misuse for TF purposes. Nonetheless, the general registration, accounting and auditing requirements applicable to all NPOs, as well as

the special money collection permit, and the associated reporting obligations, are effective transparency measures to reduce the vulnerability of NPOs at TF risk.

26. Finland implements TFS regarding PF through EU measures, which involve delays in the transposition of United Nations (UN) designations. However, in the case of Iran, the practical effect of these delays has been successfully mitigated by prior designations by the EU. In the case of the Democratic People's Republic of Korea (DPRK), a delay still exists.

27. FIs and DNFBPs have a good understanding of their TFS for PF obligations and good advice and guidance is provided by authorities. Supervisors do not have legal powers to supervise the implementation of these obligations.

Preventive measures (Chapter 5; IO.4; R.9–23)

28. FIs have an adequate understanding of their exposure to ML/TF risks, which is in line with the national picture of ML risks. However, there are some gaps on the TF side. This understanding is more developed among larger institutions or those belonging to international groups. Smaller entities such as money remitters particularly those operating “hawala” type money remittance, which are high ML/TF risks institutions, and consumer credit providers, need most improvement. The level of understanding of DNFBPs is adequate only in some sectors. In order to enhance the understanding of ML/TF risks by obliged entities, Finland should provide more risk guidance to all sectors/financial institutions. This guidance should include information on both ML and TF risk typologies, the sectors most vulnerable and red flag indicators.

29. FIs have implemented mitigation measures concerning Customer Due Diligence (CDD), record keeping and monitoring, based on relevant risks. Larger FIs or those belonging to groups have more resources to devote to their systems or can avail of group resources. DNFBPs generally apply CDD measures and take appropriate measures for higher risks including when dealing with foreign customers and Politically Exposed Persons (PEPs), and avoid dealing in cash. However, all DNFBPs experienced challenges with obtaining corporate information relating to foreigners and the beneficial ownership obligations. FIs and DNFBPs have an adequate degree of awareness of TFS regimes and of their obligations in this respect. Finland should ensure that FIs and DNFBPs enhance their ML/TF risk mitigation and control frameworks proportionate to their identified risks by providing the supervised entities with practical guidance on interpretation of the legislation and implementing preventive measures.

30. STR filing requirements are reasonably well understood by FIs. However, the number of STRs filed for some high risk FIs (for example hawala) and other sectors remains low to non-existent. There are concerns about the time delays and quality of reporting for some FIs. With the exception of gambling operators, the number of STRs reported by the DNFBP sectors is low, which is a serious concern. Finland should ensure better quality STR reporting by FIs and DNFBPs by intensifying supervisors' focus and oversight of compliance with the filing of STRs obligations and the timeliness of suspicious transaction reporting. Supervisors should liaise with the FIU to allow targeting of reporting sectors where weaknesses in suspicious transaction reporting have been identified.

31. The FIs internal control policies and procedures in place appear adequate, and no obstacles with respect to information sharing within international financial groups

have been identified. Supervisory authorities for the DNFBP sectors should provide the supervised entities with practical guidance on the application of appropriate control measures to meet the AML/CFT obligations.

Supervision (Chapter 6; IO.3; R.14, R.26–28, 34, 35)

32. A number of FIs and DNFBPs are not required to register with the relevant supervisory authority, which renders their supervision very difficult. The obligation to register only enters into force on 1 July 2019.

33. The financial supervisors apply reasonable fit and proper assessments to prevent criminals or their associates from entering into the market. However, appropriate fit and proper assessments are applied to only part of the DNFBPs.

34. The financial supervisors' understanding of ML/TF risks is inadequate for the majority of the sectors under their supervision. Their identification and understanding of the ML/TF risks specific to the sectors and FIs they supervise is more substantial for the FIs with which they have ongoing ML/TF engagement. However, this represents very few sectors within the overall population under their supervision. The DNFBP supervisors' (other than RSAA) risk understanding has not been fully aligned with the national view of risks. All supervisors should develop and adopt a methodology and process to facilitate regular and timely ML/TF risk assessment across all the sectors and obliged entities they supervise. The methodology should include both qualitative and quantitative measures to facilitate the identification and assessment of current and emerging ML/TF risks specific to the various sectors and the quality of their risk management practices.

35. Overall, the AML/CFT monitoring and supervision approach in the financial sector is not carried out on a risk-sensitive basis. The Financial Supervisory Authority (FIN-FSA) has concentrated its ongoing AML/CFT supervision on the largest banks, and has not developed an intensive supervisory approach for other high-risk institutions, such as hawalas. There is no ongoing AML/CFT supervision of lower risk firms. RSAA has concentrated its supervisory efforts on currency exchange businesses, which do not present major ML/TF risks in Finland, but has limited ongoing risk based AML/CFT supervision with other more risky sectors, such as real-estate agents. No DNFBP supervisor is able yet to conduct adequate and robust AML/CFT supervisory engagement. All supervisors should develop and adopt a risk based AML/CFT supervisory engagement model that takes into account the differing levels of ML/TF risks associated with individual FIs or DNFBPs and also each of the sectors supervised.

36. Supervisors lack powers to supervise the implementation of TFS although they do check that the necessary processes are in place when conducting the licence granting process.

37. No penalties, fines or other sanctions have been imposed on FIs and DNFBPs to date. Supervisory authorities, primarily those in charge of FIs, should be encouraged to take sanctions against supervised entities that do not comply with their AML/CFT requirements. Such sanctions should be dissuasive and reflect the severity of findings encountered.

38. Further, supervisors, and specifically FIN-FSA and RSAA, are significantly under-resourced given the breadth and depth of their AML/CFT responsibilities and

associated workload. Finland should substantially increase the resources of all supervisory authorities in order for them to be sufficiently equipped to adequately and effectively discharge their respective mandates commensurate with the varying risks and size of the diverse financial and non-financial sectors in the AML/CFT regime.

Transparency and beneficial ownership (Chapter 7; IO.5; R.24, 25)

39. Vulnerabilities involving legal persons and the potential of company misuse by criminals are generally understood. However, Finland should undertake a fully dedicated risk assessment on the misuse of all the legal persons, foreign express trusts and similar legal arrangements, as well as non-profit associations.

40. Finland has in place certain preventive measures. However, they are not effective with regard to the most risky types of legal persons. The ability of competent authorities to establish the beneficial ownership (BO) of legal persons in a timely manner is very limited. In this context, Finland should put in place robust measures to ensure the accuracy of information in all publically held registries as well as implement appropriate measures to mitigate the misuse of legal persons (such as de-registering fraudulent or dormant companies), and the activities of their front men and agents.

41. Since there is no meaningful supervision of the company service providers (see IO. 3), it leaves them open for misuse when they engage in company registration or serving as nominee directors in the companies. Finland should promote effective supervision and enforcement of BO transparency obligations, through a multi-agency approach, involving designated supervisory authorities, law enforcement agencies and other relevant authorities. The Finnish Patent and Registration Office (PRH), in charge of the trade register and other registers of legal persons, should be empowered to issue administrative sanctions for failures to submit adequate, accurate and up-to-date information, where appropriate.

International cooperation (Chapter 8; IO.2; R.36–40)

42. Finnish authorities cooperate routinely with their foreign counterparts, formally and informally, as part of their normal course of operation and the cooperation is especially close with neighbouring countries, such as Nordic countries and Estonia.

43. LEAs in particular both seek international cooperation to build their cases, and share timely and accurate information. Cooperation, including MLA requests, is generally in line with Finland's geographic risk exposure.

44. FIN-FSA, the main financial supervisor, actively engages with its counterparts for the supervision of EU and Nordic countries financial institutions/groups. Finland should nevertheless keep statistics on all its international cooperation activities related specifically to ML and TF, in order to improve its understanding of ML/TF risks.

Priority Actions

- a) Finland should ensure that AML/CFT supervisors accelerate and finalise the development of their methodology for AML/CFT supervision on a risk-sensitive basis, and implement this methodology in relation to their supervised entities as a matter of priority.
- b) Finland should allocate adequate resources to AML/CFT supervisors, and specifically FIN-FSA and RSAA, including human resources, to enable them to conduct their AML/CFT supervisory responsibilities in an adequate and effective manner.
- c) Finland should ensure that the framework in preparation for the setting up of the beneficial ownership registry requires that the information collected and stored is subject to relevant verification, and then implement the registry as a matter of urgency.
- d) Finland should ensure that the existing gaps in the common understanding of ML and TF risks are filled, and that mechanisms are in place and effectively operating to enable all relevant authorities in the country, as well as obliged entities, to have an updated and comprehensive view of ML/TF risks affecting the country.
- e) Finland should set up adequate platforms and/or channels to support operational cooperation between the relevant authorities, first of all to further improve the understanding of ML/TF risks in the country (FIU and AML/CFT supervisors), and second to leverage the potential of the FIU to produce quality financial intelligence (FIU and LEAs, especially local police departments).
- f) Finland should encourage the use of a wider range of sentences for aggravated ML cases by courts, to improve the proportionality of sentencing,

Effectiveness & Technical Compliance Ratings*Effectiveness Ratings¹*

IO.1 - Risk, policy and coordination	IO.2 - International cooperation	IO.3 - Supervision	IO.4 - Preventive measures	IO.5 - Legal persons and arrangements	IO.6 - Financial intelligence
Substantial	High	Low	Moderate	Moderate	Substantial
IO.7 - ML investigation & prosecution	IO.8 - Confiscation	IO.9 - TF investigation & prosecution	IO.10 - TF preventive measures & financial sanctions	IO.11 - PF financial sanctions	

Substantial **Moderate** **Moderate** **Moderate** **Moderate**

Technical Compliance Ratings²

R.1 - assessing risk & applying risk-based approach	R.2 - national cooperation and coordination	R.3 - money laundering offence	R.4 - confiscation & provisional measures	R.5 - terrorist financing offence	R.6 - targeted financial sanctions – terrorism & terrorist financing
LC	PC	LC	LC	LC	LC
R.7 - targeted financial sanctions - proliferation	R.8 - non-profit organisations	R.9 – financial institution secrecy laws	R.10 – Customer due diligence	R.11 – Record keeping	R.12 – Politically exposed persons
LC	PC	C	LC	C	LC
R.13 – Correspondent banking	R.14 – Money or value transfer services	R.15 – New technologies	R.16 – Wire transfers	R.17 – Reliance on third parties	R.18 – Internal controls and foreign branches and subsidiaries
PC	C	LC	C	LC	LC
R.19 – Higher-risk countries	R.20 – Reporting of suspicious transactions	R.21 – Tipping-off and confidentiality	R.22 – DNFBPs: Customer due diligence	R.23 – DNFBPs: Other measures	R.24 – Transparency & BO of legal persons
PC	C	C	LC	LC	PC
R.25 – Transparency & BO of legal arrangements	R.26 – Regulation and supervision of financial institutions	R.27 – Powers of supervision	R.28 – Regulation and supervision of DNFBPs	R.29 – Financial intelligence units	R.30 – Responsibilities of law enforcement and investigative authorities
LC	LC	PC	PC	C	C
R.31 – Powers of law enforcement and investigative authorities	R.32 – Cash couriers	R.33 – Statistics	R.34 – Guidance and feedback	R.35 – Sanctions	R.36 – International instruments
LC	LC	LC	PC	PC	LC
R.37 – Mutual legal assistance	R.38 – Mutual legal assistance: freezing and confiscation	R.39 – Extradition	R.40 – Other forms of international cooperation		
LC	LC	LC	LC		

- 1 Effectiveness ratings can be either a High- HE, Substantial- SE, Moderate- ME, or Low – LE, level of effectiveness.
- 2 Technical compliance ratings can be either a C – compliant, LC – largely compliant, PC – partially compliant or NC – non compliant.

MUTUAL EVALUATION REPORT

Preface

This report summarises the AML/CFT measures in place as at the date of the on-site visit. It analyses the level of compliance with the FATF 40 Recommendations and the level of effectiveness of the AML/CFT system, and recommends how the system could be strengthened.

This evaluation was based on the 2012 FATF Recommendations, and was prepared using the 2013 Methodology. The evaluation was based on information provided by the country, and information obtained by the evaluation team during its on-site visit to the country from 23 May to 8 June 2018.

The evaluation was conducted by an assessment team consisting of:

- Anne Karoline Bakken Staff, Senior Police Prosecutor, Norwegian Police Security Service
- Catherine Balfe, Manager, AML Division, Central Bank of Ireland
- Christopher Malan, Executive Manager Compliance and Prevention, Financial Intelligence Centre, South Africa
- Philippe De Koster, Advocate General at the Supreme court and Director FIU, Belgium
- Caroline Wänglund, AML Legal Counsel, Swedish Financial Supervisory Authority

The team was supported by the FATF Secretariat represented by Anne-Françoise Lefèvre, Pierre Bardin and Sergey Teterukov. The report was reviewed by Cindy Guadalupe Mendoza Pérez - Mexico, Darya Kudryashova - EAG/Russia and Patricia Steck-Matthews - Switzerland (scoping note).

Finland previously underwent a FATF Mutual Evaluation in 2007, conducted according to the 2004 FATF Methodology. The 2007 Mutual Evaluation report and the 2013 Exit from Follow-up report have been published and are available at www.fatf-gafi.org.

The 2007 Mutual Evaluation concluded that the country was compliant with seven Recommendations; largely compliant with 13; partially compliant with 23; and non-compliant with five (one Recommendation was not applicable). Finland was rated compliant or largely compliant with 10 of the 16 Core and Key Recommendations.

Finland was placed under the regular follow-up process, and reported back to the FATF in October 2009, October 2010, February 2011, October 2011, February 2012, June 2012 and October 2012. The FATF June 2013 follow-up report found that overall, while some deficiencies remained on SR III, Finland had made sufficient progress with respect to the Core and Key Recommendations. Finland was therefore removed from the follow-up process in June 2013.

CHAPTER 1. ML/TF RISKS AND CONTEXT

45. Finland is situated in Northern Europe, with a quarter of its total territory lying north of the Arctic Circle. Finland has land borders with Russia (east), Norway (north) and Sweden (west), and a sea border with Estonia (south). The total surface area of the country is 338 432 km², which includes the land and inland water areas and makes Finland the eight largest country in Europe.³ Seventy-five % of the land is covered by forest.⁴ The territory consists of mainland Finland and the self-governing province of Åland Islands, located in the Baltic Sea. Finnish state law applies in areas in which the Åland Parliament does not have legislative powers, that is foreign affairs, most areas of civil and criminal law, including Anti-Money Laundering/Combating Terrorism Financing (AML/CFT) legislation, the court system, customs, and state taxation.

46. Finland had 5.5 million inhabitants by the end of 2017⁵ (0.07 % of the world's population⁶) and is the most sparsely populated country in the European Union.⁷ The capital of Finland is Helsinki (640 000 inhabitants⁸). The national languages are Finnish and Swedish (about 5% of Finns speak Swedish as their native language). Finland's GDP stood at EUR 224 billion in 2017⁹, with a GDP per capita slightly above the EU average.¹⁰

47. Finland is a parliamentary democracy with a multiparty political system. It has a clear separation of powers, defined by the 1999 Constitution. The head of state is the President of the Republic, who appoints the government. Power is vested in the people, who are represented by the elected parliament. Parliament's powers include enacting laws and overseeing the operations of the government. Judicial powers are exercised by independent courts of law.

48. Finland has been a member of the European Union (EU) since 1995. Consequently, the national AML/CFT regime is based on a legal framework defined both at the EU and at national level. Finland adopted the Euro upon its introduction in 1999. Finland became a member of FATF in 1991 and it is one of the founding members of the Organisation for Security and Co-operation in Europe (OSCE) and the World Trade Organisation (WTO). Finland is also a member of other international fora such as the International Monetary Fund (IMF), the World Bank, the United Nations, the Organisation for Economic Co-operation and Development (OECD) and the Council of Europe.

3 www.worldatlas.com/articles/the-largest-countries-in-europe.html

4 <https://smy.fi/en/forest-fi/forest-facts/finnish-forests-resources/>

5 <https://findikaattori.fi/en/14>

6 www.stat.fi/ajk/satavuotiassuomi/suomiennenjanyt_en.html

7 <https://data.worldbank.org/indicator/EN.POP.DNST>

8 www.stat.fi/tup/julkaisut/tiedostot/julkaisuluettelo/yyti_fif_201800_2018_19693_net.pdf

9 <https://findikaattori.fi/en/2>

10 http://ec.europa.eu/eurostat/statistics-explained/index.php/GDP_per_capita_consumption_per_capita_and_price_level_indices

ML/TF Risks and Scoping of Higher Risk Issues

Overview of ML/TF Risks

General criminal context of Finland

49. A number of elements characterise the general criminal context of Finland:
- a) Finland is a low-crime country by international standards. Approximately 860 000 crimes were reported to Police, Customs and Border Guard in 2017¹¹ (approx. 500 000 to Police only¹²), 50% being property crimes and 25% traffic offences. There has been an overall decrease in the number of offences in recent years (-7.8% between 2010 and 2017), but the number of fraud offences has substantially increased (+38.4% between 2010 and 2017) including means of payment fraud.¹³ Organised criminals are active in Finland (about 80 groups totalling around 1 000 members), mainly as part of domestic groups (ex. motorcycle gangs).¹⁴ They are involved in narcotics-related offences, and are also expanding their activities into the construction, cleaning and restaurant sectors.
 - b) Given its geographical location, Finland is a major European gateway to and from non-European countries, and strong business and trade relationships have developed between Finland and Russia. Equally, Finland has close business ties with neighbouring Baltic States and other Nordic countries. Germany, Sweden, the US, Netherlands and Russia were Finland's biggest trade partners for goods in 2017, when measured by total volume.¹⁵ This geographic proximity supports the development of commercial routes, including trade routes in illicit flows of goods and funds.
 - c) Finnish Security Intelligence Service (SUPO) describes the threat posed by terrorism in Finland as "elevated", on a four-tier scale (low, elevated, high and severe).¹⁶ The most recent terrorist attack in Finland took place in Turku in August 2017, when a radicalised ISIL attacker stabbed 10 people (see Box 4.1). The terrorist threat has increased as radical Islamist propaganda mentioned Finland more often, and counter-terrorism target individuals have had stronger links with terrorist activities.¹⁷

Country's Risk Assessment & Scoping of Higher Risk Issues

¹¹ www.tilastokeskus.fi/tup/suoluk/suoluk_oikeusolot_en.html

¹² <https://intermin.fi/en/police/crime-in-finland>

¹³ www.tilastokeskus.fi/tup/suoluk/suoluk_oikeusolot_en.html

¹⁴ <https://intermin.fi/en/police/organised-crime>

¹⁵ <https://tulli.fi/en/statistics/international-trade-in-goods>

¹⁶ www.supo.fi/en/news/1/0/threat_assessment_unchanged_for_the_time_being_73980

¹⁷ <https://intermin.fi/en/police/counter-terrorism>

Country's risk assessment

50. Finland developed its first national risk assessment as a ML/TF risks research report, commissioned by the Ministry of Interior and independently conducted by the Police University College in 2014 (*"National AML/CFT Risk Assessment"*, NRA 2015). Relevant competent authorities and the private sector contributed. The research reviewed the threats and vulnerabilities identified by stakeholders and research material, and assessed their possible consequences. It identified six key risks items, which constitute the national risk assessment: real estate investments, transport of cash, front companies, increasing online services, online shadow financing markets and customer fund accounts. The report was published in 2015.¹⁸

51. The research was conducted in 2014 and a number of the stakeholders involved acknowledged that it does not fully reflect the ML/TF risk situation of the country today. Assessors also identified a number of methodological weaknesses, and the need to refocus the approach on the ML/TF risks of Finland, and not only on the ML/TF methods used, or potentially used, by criminals to launder crime proceeds. Finnish authorities should also adopt a global approach to turn the NRA 2015 into a shared, national reference framework for AML/CFT (see IO.1).

Assessors' views on ML/TF risks in Finland

52. In this context, assessors are of the view that the major ML risks in Finland currently relate to the following areas:

- a) The main risk of financial crime stems from the grey economy, defined as the non-payment of statutory payments like taxes, pensions, employers' payments etc.¹⁹ The grey economy is difficult to evaluate, as a large part of the shadow economy is "hidden crime" not reported to the authorities. Nevertheless, some studies estimate that the grey economy's share of Finnish GDP range from EUR one billion to 14 billion, and the economic losses for Finland caused by such non-payments range from EUR a few hundred million to five billion a year.²⁰ The main ML threat in that regard is the proceeds resulting from tax offences, which accounted for 48% of all economic crimes in 2016,²¹ as well as tax fraud.
- b) Proceeds of drug crimes are also one of the highest ML risks in Finland. Finnish authorities estimated the drug market as approx. EUR 80 million in 2014. The drug trade is dominated by domestic, organised crime groups. International connections, especially with groups based in Russia and the Baltic States, are used to bring narcotic products into

18

www.theseus.fi/bitstream/handle/10024/97954/Raportteja_117_verkko.pdf?sequence=1&isAllowed=y, EN summary p. 113

19 [National strategy for tackling grey economy and economic crime 2016/2020](#)

20 www.vero.fi/en/grey-economy-crime/scope/estimates-on-the-shadow-economy-and-tax-gap; <https://intermin.fi/en/police/economic-crime-and-the-shadow-economy>

21 <https://intermin.fi/en/police/economic-crime-and-the-shadow-economy>

Finland²². Cash is often involved in those transactions, and virtual currencies have been increasingly used in recent years.²³

- c) Proceeds from both domestic and foreign frauds are the other highest ML risks in Finland. Frauds of various kinds have been identified, in addition to fraud involving tax evasion (see above). They include for example fraud associated with accounting offences, or card-payment abuse and increasingly, internet-based fraud. Mass marketing fraud for example, involved transactions worth almost EUR 12 5 million between 2012/17, and in some individual cases, the crime proceeds were more than EUR 250 000.

53. A significant part of the proceeds generated in Finland is moved out of the country. Destination countries vary depending on the type of predicate offences involved, but neighbouring countries such as the Baltic States, and especially Estonia, are primary targets. Drug money tends to flow to Southeastern Europe/Western Asia, especially Turkey, but also to EU countries such as Spain or the Netherlands. Large parts of the proceeds from mass-marketing fraud cases are also transferred to African countries.

54. Main ML methods are the use of front companies, complex corporate structures and front persons, in particular in grey economy-related cases. The construction sector is one of the major business activities where such methods have developed. In most cases, family or close acquaintances are involved as strawmen. Although some professional intermediaries might contribute to setting up asset-concealing schemes involving several layers of corporate entities, with international, and possibly offshore, connections, this does not seem to be standard practice in Finland.

55. Cash couriers, mainly in connection to drug money (see above), and wire transfers are other channels predominantly used in Finland to move proceeds out of the country.

56. The main TF risks stem from sympathisers of terrorist cause and Foreign Terrorist Fighters (FTFs) in particular, and returned FTFs. The returnees as well as lone wolves, who have not left Finland, make up the most significant terrorism and TF threat in Finland. The main TF methods used are money transfers, including through registered and unregistered hawalas, and misuse of Non-Profit Organisations (NPOs).

Scoping of Higher Risk Issues

57. In deciding what issues to prioritise during the on-site visit, the assessment team reviewed material provided by Finland on national and cross-border ML/TF risks, and information from reliable third party sources (e.g., reports by international organisations). The items below were listed in the scoping note, which was submitted to Finnish authorities prior to the assessment team's on-site visit.

²² [https://intermin.fi/en/police/organised-crime;
www.emcdda.europa.eu/countries/drug-reports/2017/finland/drug-markets_en](https://intermin.fi/en/police/organised-crime;www.emcdda.europa.eu/countries/drug-reports/2017/finland/drug-markets_en)

²³ <https://intermin.fi/en/police/organised-crime>

They include potential areas of higher ML/TF risks, as well as issues that were of concern to the assessment team or where further clarification was sought.

- a) *Geographical location and business relationships with neighbouring countries*, and the impact on money flows, especially from outside the EU, including money transfers and cash transportation.
- b) *The grey economy and tax evasion/fraud*, and interaction with the national AML/CFT policy, as well as typologies on how the proceeds from grey economy-related offending and tax crimes are generated and laundered.
- c) *Supervisory resources and framework*, and sanction regimes available to supervisors, as well as clarification of the 2017 changes to the Designated Non-Financial Businesses and Professions (DNFBPs) supervisory regime (see 1.2.6 below and IO.4).
- d) *FIU functions as a police-type body*, and specifically FIU responsibilities at the intelligence gathering and analysis stages, as well as the FIU operational independence.
- e) *Transport of cash*, in particular through the use of cash couriers at the internal EU borders.
- f) *Hawala-type institutions*, in particular measures put in place to supervise registered firms and eventually identify unlicensed/unregistered firms.
- g) *NPO sector*, with a focus on TF risks.
- h) *Vulnerable DNFBP sectors*, including the real estate, gambling and precious metals and stones sectors.

Materiality

58. Today, the largest sector of the Finnish economy is services (65 %), followed by manufacturing and refining (31 %).²⁴ Traditional branches of industry have remained, and Finland is still one of the world's leading wood producers.²⁵ The 2008 world trade slowdown hit exports and domestic demand hard, along with the economic downturn of Russia - where 10% of Finnish exports were directed-, and the decline of the paper industry and of the national electronics/technology champion. Finland's economy contracted from 2012 to 2014, but returned to growth in 2015, posting a 2.1% GDP increase before growing to 2.6% in 2017.²⁶

59. Finland had been one of the best performing economies within the EU before 2009 and its banks and financial markets avoided the worst of the global financial

²⁴ www.oecd.org/finland/

²⁵ www.forestindustries.fi/statistics/

²⁶ Ministry of Finance figures (presentation made during the on-site)

crisis. The financial sector in Finland is dominated by the banking sector, with a ratio to GDP at approximately 200%.²⁷

60. Finnish society is highly banked, with 18 million deposit accounts in 2016, which translates to an average of about three payment accounts per person. Finland is characterised by a relatively low use of cash, which has decreased as a means of payment with the introduction of new payment methods and the increase of online trade. The ratio of cash payments to card payments is approximately 20-80%²⁸, and the total value of cash payments has fallen by almost 50% since the 2000s (from approx. EUR 32 million to EUR 15 million).

61. The Finnish welfare state model involves significant levels of taxation and social payments. In that context, reducing the grey economy and economic crime is a major national policy priority, and has been the subject of several multi-year strategies since the end of the 90's (see below on AML/CFT Strategy). This has a major impact on the focus and priorities of the country's AML activities.

Structural Elements

62. The key structural elements needed for an effective AML/CFT regime are present in Finland. It is a politically and institutionally stable country, based on accountability, transparency and the rule of law. Responsibility for developing and implementing AML/CFT policy in Finland is shared between relevant authorities, whose statutes and roles are well defined.

Background and Other Contextual Factors

AML/CFT strategy

National Strategy to tackle the grey economy and economic crime

63. Finland is built on a strong social market economy and welfare state model, which involves comparatively high levels of taxation and social payments.²⁹ In that context, reducing the grey economy and economic crime is a major national policy priority. These actions target the non-payment of statutory taxes, social security, pension or other payments and contributions required by law.

64. Tackling the grey economy and economic crime has been the subject of national strategic plans since 1996, and is a collaborative effort between authorities, coordinated by the Ministry of Interior. Actions are driven by a Steering Group³⁰, which reports to the Ministerial Committee on Economic Policy, supported by a

²⁷ www.esrb.europa.eu/pub/rd/html/index.en.html; <http://sdw.ecb.europa.eu/reports.do?node=1000003229>. This ratio has significantly raised since October 2018 and the move of Nordea headquarters to Finland, see 1.2.3.a

²⁸ AML Action Plan, Section 4.2.

²⁹ www.oecd-ilibrary.org/docserver/eco_surveys-fin-2018-en.pdf?expires=1530781616&id=id&accname=ocid84004878&checksum=F5D45608D2EA3D9B7DD3D0DA5C0135B0, see figure 16, p. 34

³⁰ Steering Group members include representatives of the Ministries of Economic Affairs and Employment, of Social Affairs and Health, of Finance, Finnish Competition and Consumer Authority, Ministry of Justice, Office of the Prosecutor General etc.

dedicated Tax Administration Unit (Grey Economy Information Unit) set up by law in 2011, and monitored by a parliamentary group. A website has recently been launched to remind the public that combating the grey economy and economic crime is a collective responsibility, which benefits all -authorities, companies and citizens.³¹

65. The strategic initiatives are tailored to areas where the grey economy is prevalent, and the major objectives include increasing transparency of businesses and facilitating companies' compliance with their statutory obligations. For example, additional tax obligations were imposed on the construction sector, including: a reverse charge for the payment of VAT (2011); an individual tax number for all workers, including foreign workers, as well as their registration in a single register as taxpayers before they start working (2012); and a duty to notify all construction contracts and workers to the Tax Administration (2014). The 2015 increase by about EUR 100 million of the revenue of wage taxes in the construction sector illustrates the positive effect of these initiatives.

66. Finland also established a tax debt register at the end of 2014 which allows anyone to check outstanding tax liabilities (of at least EUR 10 000) and non-filing of tax returns of all types of companies, self-employed individuals and estates operating a business. There is an obligation to check this register before concluding a contract on temporary agency work or subcontracted labour. In the construction sector, this measure, combined with effective labour inspection activities and co-operation with sectoral social partners, resulted in a substantial decrease in the share of inspected contracts subject to negligence fees process (20% in 2013, to 8-10% in the last years).³²

67. The 2016/2020 National Strategy to tackle Grey Economy and Economic Crime was adopted through a government resolution in April 2016.³³ It focuses heavily on preventive measures and co-operation between relevant authorities. The Strategy is supported by an Action Plan that identifies 20 initiatives in 4 strategic areas: promoting healthy competition between companies, preventing the grey economy and economic crime, improving public authorities' co-operation and strengthening sanctions related to the grey economy.

68. As part of the measures to enhance further the co-operation between authorities, wider access to "Compliance reports" was agreed, entering into force in June 2018. Compliance reports have been in place since 2011 as analytical reports of information and data held in the different databases of Finnish administrations (e.g. tax, debt collection, fund granting, business register, financial statements, business connections and ownership etc.) on all legal entities or associated persons and the management that engage in commercial activities in Finland. They provide a comprehensive overview on how this person or entity complies and has complied with legal obligations concerning tax and other statutory payments, fees charged by Finnish Customs, business activities, financial position and connections. These reports are produced through a mostly automated mechanism and provided by the

³¹ www.vero.fi/en/grey-economy-crime/

³² Tax Administration figures (presentation made during the on-site)

³³ https://intermin.fi/en/article/-/asset_publisher/harmaata-taloutta-ja-talousrikollisuutta-voidaan-parhaiten-torjua-ennalta-estavalla-tyolla

Grey Economy Information Unit (GEIU) to requesting authorities. Twenty-three public authorities have access to these reports, including the FIU, Police, Customs, etc. The financial supervisor (FIN-FSA) was recently added. The GEIU received almost 275 000 requests for Compliance reports in 2017 (192 613 in 2016 and 161 270 in 2015)³⁴ (see also IO.6).

69. As part of the 2016/20 National Strategy on the Prevention of the Grey Economy, an AML Action Plan was adopted on 8 June 2018. Measures to address and mitigate the six key risk items (see section above) are outlined, most of which relate to the legislative framework.

Counter terrorism strategy

70. The National Counter-Terrorism (CT) Strategy was adopted in 2014, and updated in June 2016. It was a four-year plan, adopted as a follow-up to the 2010-2014 strategy, and set priorities for 2014-2017. The main pillars of this strategy were prevent, pursue, tackle and respond to the terrorism threat. An action plan supported the CT strategy, which focused on prevention and included fighting terrorism financing.

71. It is noted that the draft government decision on the National Counter-Terrorism Strategy 2018-2021 is under review and expected to be adopted during the autumn of 2018.

Legal & institutional framework

AML/CFT/CPF Institutional framework

Relevant Ministries

- a) *Ministry of the Interior* is the lead ministry for AML/CFT. It chairs the FATF Steering Committee and AML/CFT Co-ordination Group (see below), and is in charge of AML/CFT legislation. It also directs the National Police Board (see below), which in turn is in operational command of all police forces.
- b) *Ministry of Finance* is in charge of the financial sector legislation, which includes AML/CFT preventive measures and supervisory arrangements applicable to financial institutions (except insurance, which is the responsibility of the Ministry of Social Affairs and Health).
- c) *Ministry of Economic Affairs and Employment* is responsible for the legislation on the trade register, accounting and auditing, as well as the economy, business environment and employment matters in general.
- d) *Ministry of Justice* is in charge of the legislation on criminal law, as well as on company law and law on associations and foundations. It also plays a central role in mutual legal assistance.

³⁴ Tax Administration figures (presentation made during the on-site)

- e) *Ministry for Foreign Affairs* is responsible for the legislation on international sanctions, including targeted financial sanctions on TF and PF, and coordinates activities related to CPF.
- k) *Relevant supervisory authorities and self-regulatory bodies*
- f) *Financial Supervisory Authority (Finanssivalvonta or FIN-FSA)* comes under the authority of the Ministry of Finance, and is administratively part of the Bank of Finland, although it operates independently. It is in charge of the supervision of Finland's financial and insurance sectors, including for AML/CFT.
- g) *Regional State Administrative Agency for Southern Finland (Aluehallintovirasto, AVI or RSAA)* - There are six regional state administrative agencies in Finland, whose mission is to ensure regional equality by promoting legal protection and healthy and safe living conditions, including through supervisory tasks laid down in the law. RSAA has a national competence to act as the AML/CFT supervisor for a range of financial institutions and DNFBPs (see Tables 1.1 and 1.2).
- h) *Finnish Patent and Registration Office (Patentti – ja rekisterihallitus or PRH)* is under the authority of the Ministry of Economic Affairs and Employment and is in charge of registering companies, associations, foundations, religious organisations, and maintains the relevant registers.
- i) *National Police Board/Gambling Administration (NPB/GA)*³⁵ is in charge of supervising mainland-gambling operators from an AML/CFT perspective. NPB/GA also grants money-collection permits to NPO organisations, and oversees the application of the Money Collection Act (see Box 4.7).
- j) *Finnish Bar Association* is a self-regulatory body in charge of the AML/CFT supervision of Bar attorneys, who do not include all lawyers active in the country (see Table 1.2).

Criminal justice and operational agencies

- k) *Financial Intelligence Unit (FIU)* is placed in the National Bureau of Investigation (NBI), which is part of the Police, and acts as an operationally independent unit.
- l) *National Police Board (NPB)* is under the direction of the Ministry of the Interior. Its tasks include planning, directing, developing and supervising police operations and the related support functions conducted by the 11 Police Departments, the National Bureau of Investigation and the Police University College. The vast majority of criminal investigations into predicate offences and related ML as well as TF are conducted by the Police (see IOs 7 and 9).

³⁵ Regarding the gambling operators of Åland, a Presidential decree has transferred the competence from the NPB/GA to the gambling supervisory authority in Åland. This decree entered into force on 1 July 2018 and is therefore not part of this mutual evaluation.

- m) *Customs* is under the responsibility of the Ministry of Finance and has responsibility for the control of imports and exports, international traffic, and customs and excise duties, as well as for control of cash entering or leaving the Finnish territory. It has investigative powers for customs offences and related ML or TF offences.
- n) *Border Guard* operates under the Ministry of Interior. Tasks include guarding Finland's borders on land and at sea, and carrying out border checks at land border crossing points, ports and airports. Because Finland is an EU Member State and a Schengen area country, activities focus on the external border. It has investigative powers for offences related to its duties.
- o) *Tax Administration (FTA)* conducts administrative investigations on tax matters. These investigations can reveal suspected tax offences, which are one of the main ML predicate offences in Finland (see Chapter 1). FTA's Corporate Taxation Unit has specialised personnel on the grey economy who conduct tax audits and other control measures, often together with Police.
- p) *Finnish Security Intelligence Service (Suojelupoliisi or SUPO)* is a national police unit operating under the Ministry of the Interior. SUPO's core functions are counter intelligence, counter terrorism, and security work.
- q) *Prosecution service* – The Office of the Prosecutor-General is the central administration for the prosecution service. It is also responsible for the prosecution of terrorist offences.
- r) *National Administrative Office for Enforcement* is in charge of the administrative management, guidance and supervision of enforcement authorities.
- s) Enforcement tasks are carried out by *local (district) enforcement offices* (bailiffs), responsible for handling seized proceeds of crime and terrorist funds and for enforcing court decisions, tax debts, public charges, fines, etc.; and *special enforcement offices*, such as the Helsinki Special Enforcement unit responsible for implementing targeted financial sanctions (TFS) freezing.

AML/CFT/CPF Legal framework

72. Finland's legal framework for AML/CFT is set out in the AML/CFT Act (444/2017) and FIU Act (445/2017). The crime of ML is defined in the Criminal Code (Chapter 32, sections 6 to 9) and meets many of the requirements of the Vienna and Palermo Conventions (see TC Annex, R. 3). The crime of TF is also defined in the Criminal Code (Chapter 34(a)), on the basis of the Terrorist Financing Convention, but some technical deficiencies are noted (see TC Annex, R. 5).

73. The CPF framework of Finland is based on the relevant EU Regulations (Council Decision 2016/849 and Regulation 2017/1509 for DPRK; Council Regulation 267/2012 as amended by Regulations 2015/1861 and 1862 for Iran).

AML/CFT/CPF Co-operation and co-ordination mechanisms

74. The FATF Steering Group, set up in 2015 and led by the Ministry of Interior, is responsible for ensuring co-operation and co-ordination between national authorities for the prevention of ML/TF and the development of action plans against ML and TF. The National Co-ordination Group on Combating ML and TF (“AML/CFT Co-ordination Group”) was set up in May 2018 with a view to provide a platform for operational co-ordination between the FIU, supervisors and law enforcement authorities (see IO.1).

75. The Sanctions Co-ordination Working Group chaired by the Ministry of Foreign Affairs (MFA) is responsible for co-ordinating questions relating to the financing of the proliferation of weapons of mass destruction. The MFA is the competent authority for PF-related issues, with the Unit for Arms Control responsible for non-proliferation and the Unit for Public International Law responsible for sanctions, including PF-sanctions.

*Financial sector and DNFBPs**Financial sector***Table 1.1. – Financial institutions subject to the AML/CFT Act**

Institutions in **red** are not financial institutions within the FATF meaning (FATF Glossary) and as such will not be considered in the MER.³⁶

Type of Entity	N° of entities Licensed / Regulated / Registered (2017)	AML/CFT Supervisory authority/self-regulatory body	Governing legislation
Credit institutions	269	FIN-FSA	Act on Credit Institutions
Payment institutions (including e-money institutions)	11 (including 1 authorised e-money payment institution)	FIN-FSA	Act on Payment Institutions
Registered payment service providers (without authorisation, under waiver regime of the Payment Services Directive)	42 (including 18 money remitters and 6 registered e-money issuers)	FIN-FSA	Act on Payment Institutions
MVTS/money remitters	18 (money remitters under FSA’s supervision, of which 14 hawala-type firms)	FIN-FSA	Act on Payment Institutions
Agencies of foreign payment institutions	8	FIN-FSA	Act on Payment Institutions

³⁶ There are two specific financial institutions whose ongoing supervision is in the remit of the FIN-FSA, but their licencing is formally within the authority of the Ministry of Finance. These are the Helsinki stock exchange and the Finnish Central Securities Depository Ltd. They have existed in the market since many years and now belong to international financial groups. For this reason, they will not be considered in this MER.

Type of Entity	N° of entities Licensed / Regulated / Registered (2017)	AML/CFT Supervisory authority/self-regulatory body	Governing legislation
Fund management companies	26	FIN-FSA	Act on Common Funds
Alternative Investment Funds Managers (authorised and registered)	109	FIN-FSA	Act on Alternative Investment Fund Managers
Investment firms	66	FIN-FSA	Act on Investment Services
Non-Life insurance companies	36	FIN-FSA	Insurance Companies Act
Life Insurance companies	10	FIN-FSA	Insurance Companies Act Act on Foreign Insurance Companies
Insurance brokers	84	FIN-FSA	Act on Insurance Mediation
Mutual insurance associations	5	FIN-FSA	Local Mutual Insurance Associations Act
Crowdfunding intermediaries	2	FIN-FSA	Crowdfunding Act
Intermediaries of Consumer Credit Relating to Residential Property	0	FIN-FSA	Act on Intermediaries of Consumer Credit Relating to Residential Property
Consumer credit providers	49	RSAA	Act on the Registration of Certain Credit Providers and Credit Intermediaries
Other financial service providers supervised by the RSAA	2500 (estimated)	RSAA	AML/CFT Act
Currency exchange providers	16	RSAA	AML/CFT Act

Source: Finnish authorities

76. Some types of financial institutions (referred to as “other financial service providers”) are not under a legal requirement to register, hence for some activities, it is difficult for national authorities to know exactly how many providers operate. This category includes other credit lending and financial services (like financial leasing, corporate loans etc.), holders of debt collection permits or pawnbrokers.

77. The Finnish banking landscape went through two major developments over recent months, which affected the largest banking institutions in the country:

- The Danske Bank Finnish subsidiary merged with its Danish parent company at the end of 2017, resulting in Danske now operating as a branch in Finland.

- In March 2018, Nordea Bank AB took the decision to move its headquarters from Sweden to Finland³⁷.

78. The market remains dominated by domestic or Nordic-based conglomerates. Another special characteristic of the Finnish banking sector is the percentage of foreign branches and subsidiaries, which amounts to almost two thirds of the banking sector's balance sheets.³⁸ As part of the EU Single Supervisory Mechanism, Finland counts three significant banking entities (Nordea Bank AB, OP Osuuskunta, and Kuntarahoytus Oyj) under the direct prudential supervision of the European Central Bank (see section on Supervisory Arrangements).

79. The banking sector is highly concentrated. The three credit institutions hold 71.5% of loans and 77.3% of deposits at the end of 2017.³⁹ Finland's banking sector has a solid financial standing,⁴⁰ although experts say that the relocation of Nordea increases the banking sector's exposure to structural vulnerabilities due to its increased concentration and the interlinks between the market players.⁴¹

80. In Finland, payment services are offered by credit and payment institutions, as well as registered payment service providers. They forwarded payments worth approximately EUR 74 million in 2016. Amongst the 18 money remitters operating in Finland under FIN-FSA's supervision, 14 are hawala-type firms, which are AML/CFT obliged entities. Some money transmission is happening in the unauthorised space. Although the fund capital of investment funds has grown greatly over the last few years, it remains small compared to other countries, and extremely concentrated.⁴²

81. Peer-to-peer intermediaries/companies mediating peer-to-peer loans are traders, which mediate credits to consumers when the credit provider is, in most situations a private party but could also be a consumer credit company, for example. In most cases, these platforms provide payment services to participants and therefore are also payment service providers falling within the scope of FATF financial activities. Crowdfunding intermediaries provide lending-based crowdfunding to corporate customers, as well as investment-based crowdfunding with financial instruments falling within the scope of the markets in financial instruments EU Directive (MiFID), offered by some banks and investment firms. Because crowdfunding intermediaries often also provide payment services, they fall within the scope of financial institutions in the FATF meaning.

³⁷ The move took place on 1st October 2018, after the end of the onsite visit.

³⁸ <https://sdw.ecb.europa.eu/servlet/desis?node=1000004033>

³⁹ Bank of Finland – loans and deposits without monetary financial institutions

⁴⁰ www.bankingsupervision.europa.eu/banking/statistics/html/index.en.html

⁴¹ www.bofbulletin.fi/en/2017/articles/financial-stability-assessment-finland-s-banking-sector-expands-banking-union-mitigates-risks/

⁴² www.suomenpankki.fi/en/Statistics/investment-funds/

DNFBP sectors

Table 1.2. – DNFBPs subject to the AML/CFT Act

Auditors and tax consultants (in red in the table below) are not DNFBPs within the FATF meaning (FATF Glossary) and as such will not be considered in the MER.

Type of Entity	N° of entities Licensed / Regulated / Registered (2017)	AML/CFT Supervisory authority/self-regulatory body
Trust and Company Service Providers	58	RSAA
Casinos/ other gambling falling within the scope of the Recommendations	1 (mainland) 1(Åland)	National Police Board/Gambling Administration ⁴³
Attorneys (members of the Finnish Bar Association)	2 100 attorneys and 800 law firms	Finnish Bar Association
Legal service offices	840 (estimated)	RSAA
Accountants	4294	RSAA
Auditors	1 498	Finnish Patent and Registration Office (PRH)
Tax consultants	4 837	RSAA
Precious Metals & Stones Dealers	850 (estimated)	RSAA
Real estate agents	1 797 (mainland) 18 (Åland)	RSAA ⁴⁴
Notaries	N/A	

Source: Finnish authorities

82. A number of DNFBPs are not under a legal requirement to register hence for some activities, it is difficult for national authorities to know exactly how many providers operate (ex. high-value goods dealers and legal service offices).

83. Finland has diverse DNFBP sectors, which extend to dealers in goods who transact in cash above EUR 10 000 (which, in addition to precious metals and stones dealers, covers motor vehicle dealers, boat dealers, antiques and art dealers, fur and leather wholesalers, clock and jewellery shops, and auctioneers). Accountants, lawyers or other independent legal professionals, as part of their general service offer, may provide corporate formation services and business address services. While trust formation services do not exist, accountants, auditors and legal professionals may provide trust administration services to foreign express trusts in Finland. Auditors generally provide auditing, corporate and taxation law services, and do not engage in company services on behalf of their clients.

84. There is one casino in mainland Finland (which is wholly owned by the government of Finland) and one in Åland Islands (wholly owned by the regional government of Åland), which also offers online gaming (70% of total operations) and ship-based gaming activities (30 cruise ferries to/from Spain, Estonia, Latvia, Sweden).

85. In Finland, there is no monopoly in assisting in court proceedings. Lawyers who advise on and assist in legal matters are divided into two categories: members of the Finnish Bar Association (“attorneys-at-law”) and non-members of the Bar

⁴³ For the Åland casinos and gaming operations, the Presidential decree transferring the competence from the NPB/GA to the Gambling Supervisory Authority in Åland has entered into force on 1st July 2018.

⁴⁴ For the Åland-based real estate agents, the Presidential decree transferring the competence from the RSAA to the Government of Åland has entered into force on 1st July 2018.

(“lawyers” in legal service offices). Those two different categories of legal counsels are equally required to comply with AML/CFT requirements, but supervisory authorities differ (see Table 1.2).

86. There is a wide range of professionals offering accounting services, from big companies, which are parts of international networks and provide different types of company support services, to one-person offices specialised in accounting services. Nearly all corporations and foundations in Finland are required to keep accounting records, as are natural persons engaged in business or professional activities. Finnish accounting firms may not perform both accounting (compilation of financial statements) and audits for the same business, as independent auditors conduct auditing separately.

87. Dealers in precious metals and stones cover a wide range of diversified activities such as wholesale or retail jewellery shops or pure metal dealers such as bullions, or gold retailers. They are obliged entities in so far as they accept cash payments beyond EUR 10 000.

88. Real estate agents, as well as rental accommodation brokers are subject to AML/CFT requirements. There are a large variety of players as some real estate agents are part of regional or national real estate networks or groups, which cover various real estate activities (e.g. property development, or construction), or are involved in financing activities (e.g. banking groups or conglomerates). Others are one-person or smaller businesses, for whom real estate transactions are the only focus. Real estate transactions have increased by 17% since 2013, and reached EUR 8,3 billion in 2017, with 1,2% of properties bought by foreign nationals (1,1% in value of transactions)⁴⁵, a proportion which is decreasing (see IO.1).

89. There are no “notaries” in Finland who perform the activities targeted by the FATF.⁴⁶

Materiality and level of ML/TF risks of the different FIs and DNFBPs

90. The assessors ranked obliged sectors on the basis of their relative importance in the Finnish context given their respective materiality and level of ML/TF risks. The assessors used these rankings to inform their conclusions throughout this report, weighting positive and negative implementation issues more heavily for important sectors than for less important sectors. This approach applies throughout the report, but is most evident in IO.3 and IO.4:

- a) **most significant:** banking sector based on the overall market share, as well as known ML/TF typologies, and hawala-sector based on known cases of abuse for TF and insufficient supervision;
- b) **significant:** casinos, real estate agents, accountants and legal services providers (both attorneys and independent legal service providers) based on exposure to ML/TF risks and lack of AML/CFT supervision, and MVTs providers based on substantial exposure to ML/TF risks, and numerous cases of abuse;

⁴⁵ National Land Survey of Finland (presentation made during the on-site)

⁴⁶ www.maistraatti.fi/en/Services/notary_public/

- c) **less significant:** other financial institutions, including securities providers and insurance and other DNFBPs.

Preventive measures

91. Finland's legal framework for AML/CFT was revised in 2017, with the entry into force in July of a new AML/CFT Act (444/2017) and FIU Act (445/2017). The AML/CFT Act was further amended in spring 2018 (406/2018), and the relevant measures entered into force on 5 June 2018. Those measures have introduced the requirements of the 4th EU Money Laundering Directive (2015/849) in Finnish Law.⁴⁷

92. The scope of the AML/CFT Act is wider than the FATF Recommendations, partly on a risk-sensitive basis. It extends to non-life insurance activities, and to a broader range of gambling services, as the CDD requirements of the AML/CFT Act apply to all gambling services (with the exception of slot machines kept outside casinos), with no minimum amount.

93. Based on the requirements of the 4th AML Directive, the AML/CFT Act also applies to auditors and tax advisors.

94. In Finland, legal texts adopted by the Parliament include extensive legal reasoning explaining the background, objective and meaning of the provisions. These explanatory memoranda (*hallituksen esitys, HE* in Finnish)⁴⁸ are the main source of interpretation of the law because they provide information on the legislator's intention. Reasoning and guidance provided in the explanatory memoranda are closely followed by people applying the legal provisions (for example officers with power of arrest, prosecutors and judges).

Legal persons and arrangements

Table 1.3. - Overview of legal persons in Finland

Type of Legal Persons	N° of registered entities
Companies and businesses, of which:	619 104
- Limited liability companies	275 006
- Partnerships	37 892
- Cooperatives	4 287
- Mutual insurance companies	32
- Savings banks	19
- Mortgage societies	1
- Insurance associations	7
- Right-of-occupancy associations	17
- European Economic Interest Groupings	1
- Societas Europaea	1
Associations	106 001

⁴⁷ The 5th EU Money Laundering Directive was adopted and entered into force on 9 July 2018. Member States have until 20 January 2020 to implement the new rules in their national legislation.

⁴⁸ Referred to as "Government proposals" in the 2007 MER, see para 9

Type of Legal Persons	N° of registered entities
Foundations	2 706
Religious communities	473

Source: Finnish authorities

95. The most common types of legal persons in Finland are limited liability companies, partnerships and co-operatives.⁴⁹ All three types, as all other businesses established in Finland, have to be registered with the Finnish Patent and Registration Office (PRH) and basic information on them can be accessed through the trade register.⁵⁰

96. *Limited liability companies* may be private or public; only public companies can turn to the public to raise capital. One or several founders, physical person or legal person, may establish a limited liability company. The articles of association (filed with PRH and public document), specify the basis for the company's activities. The managing director, and as a rule, at least one the board members, and at least one of the deputy members must be resident within the EEA.

97. *Partnerships* exist as trading partnerships and limited partnerships. In a trading partnership, partners are personally responsible for the company's contracts and debts. In a limited partnership, there has to be at least one partner with unlimited responsibility. The agreement to establish the partnership can be made in writing or orally. In practice, it has to be made in writing and signed by all the partners because it has to be registered at PRH. At least one of the partners in a general partnership or of general partners in a limited partnership has to have a place of residence or, if the partner is a legal person, the registered office in the EEA.

98. *Co-operatives* are formed by a minimum of three physical persons or legal entities. For a co-operative to acquire legal capacity, it must be registered with PRH. After a co-operative has been registered, its liability extends only to the capital assets contributed by its members. The managing director, and as a rule, at least one the board members, and at least one of the deputy members must be resident within the EEA.

99. Non-Profit Associations, foundations and religious communities have to be registered in the relevant public registers available from and maintained by PRH.

100. *Non-profit associations* - If an association conducts business, it should, in certain circumstances, also be registered in the Trade Register. Non-profit associations are used, as a legal form, by a range of organisations including trade unions, employers' associations, charities, sports associations, voluntary organisations, political parties, etc. Membership in a non-profit association does not entitle an individual to any form of ownership of the association's assets.

101. *Foundations* - A foundation deed must be established in writing and signed by the founders. An authorised auditor is compulsory for all foundations. Foundations with a "qualified public benefit" purpose may qualify for beneficial tax treatment.

102. *Religious Communities* refers to the Evangelical Lutheran and Orthodox Church and to a religious community registered in compliance with the Freedom of

⁴⁹ A description of other types of legal persons is available in the TC Annex, R. 24

⁵⁰ www.prh.fi/en/kaupparekisteri.html

Religion Act 453/2003. The purpose of a religious community is to organise and support the individual, community and public activity relating to the professing and practising of religion, which is based on confession of faith, scriptures regarded as holy or other specified, established grounds of activity regarded as sacred. The community shall realise its purpose respecting basic and human rights. The purpose of the community is not to seek economic profit or otherwise organise mainly economic activity. A community may not organise activity for which an association within the meaning of the Associations Act (503/1989) would not be able to be founded or for which an association would only be able to be founded subject to permission.

103. As far as *legal arrangements* are concerned, express trusts or other comparable legal arrangements cannot be established under Finnish law. However, trusts or other comparable legal arrangements created under and governed by foreign law can perform business activities in Finland. There is no information available on the number of such legal arrangements.

Supervisory arrangements

104. Finnish financial institutions are supervised by two supervisors for AML/CFT: the Financial Supervisory Authority (FIN-FSA) and the Regional State Administrative Agency for Southern Finland (RSAA), see Table 1.1 The recent market developments in the Finnish banking sector (see section on Financial Institutions and DNFBPs.) resulted in Danske Bank's Finnish branch being under the supervision of the FIN-FSA.

105. Under the EU Single Supervisory Mechanism (SSM), in force since November 2014, the European Central Bank (ECB) is the authority in charge of all banking authorisations in the euro area, whether banks are large or small. It is also responsible for the supervision of Significant Institutions (SIs),⁵¹ which are the three large credit institutions in Finland (see section on Financial Institutions and DNFBPs).⁵² This involves the review of fit and proper requirements, but AML/CFT supervision is conducted by national supervisors (see IO.3).

106. The DNFBP sectors are supervised for AML/CFT purposes by RSAA and National Police Board/Gambling Administration (NPB/GA), with the exception of Bar attorneys who are supervised by the Bar Association, which is a self-regulatory body (SRB), see Table 1.2. Regarding the gambling operator and real-estate agents in Åland Islands, it is noted that a Presidential decree will transfer the competence from the NPB/GA to the Gambling supervisory authority in Åland (*Lotteriinspektion*), and from RSAA to the Government of Åland for real estate agents.⁵³

International co-operation

107. Due to its geographic location, Finland has close socio-economic ties with other Nordic countries (Denmark, Norway, Iceland and Sweden), but also with the Baltic States and Russia. It is also closely connected to other EU countries, and

⁵¹ www.bankingsupervision.europa.eu/about/thessm/html/index.en.html

⁵² www.bankingsupervision.europa.eu/ecb/pub/pdf/ssm.list_of_supervised_entities_201806.en.pdf

⁵³ The Presidential decree transferring the competence entered into force on 1st July 2018.

specifically with its main trading partners such as Germany and the UK. The US is also one of its main commercial partners.

108. Cross-border co-operation, co-ordination and information sharing with other Nordic countries and EU Member States is facilitated by various Nordic-wide or EU-wide processes based on equivalent treatment or simplified procedures (e.g. extradition between Nordic countries), or dedicated structures (e.g. EU supervisory colleges).

109. Various bilateral, multilateral and supranational mechanisms are also available to Finnish authorities. For example, the National Bureau of Investigation (NBI) uses both the Europol and Interpol channels of communication for exchanging information with foreign counterparts (Siena platform, I-24/7 global police communications system). The FIU has signed 37 MoUs with its counterparts in third countries to facilitate AML/CFT co-operation. Customs authorities co-operate through the 22 agreements in force (one is waiting for implementation).

110. With Nordic countries, as well as with EU Member States, co-operation, including mutual legal assistance (MLA) and extradition, usually occurs through direct contact between relevant authorities. With non-Nordic and non-EU countries, there is an MLA single point of contact (SPOC) which is the Ministry of Justice, including for extradition, and in practice, the request is presented by a prosecutor.

Key Findings and Recommended Actions

Key Findings

- a) Finland has an adequate understanding of its economic crime risks, and of its main ML risks, associated to the grey economy. The National Strategy on the Prevention of the Grey Economy and Economic Crime sets a relevant framework to address the main identified ML risks in a coordinated manner and puts forward an efficient preventive approach to economic crime.
- b) Other major ML risks identified in Finland – drugs and frauds – are adequately addressed by Finnish authorities, based on mutually supportive actions between relevant authorities.
- c) The understanding of ML risks, and of ML channels, is nevertheless uneven across Finnish authorities, and there are specific concerns regarding supervisors' overall understanding of ML risks.
- d) Key national authorities for combating TF have a sound understanding of TF risks. They address the identified TF risks in a manner which is consistent with the nature and level of TF risk in the country.
- e) The AML/CFT priorities and activities of the law enforcement community, intelligence and tax authorities are aligned with the national risk picture. However, supervisors' ML/TF risk-driven objectives and activities are limited.
- f) Finland conducted its first research on ML/TF risks in 2014/15 ("NRA 2015") and will be reviewed to reflect the evolution of ML/TF risks and mitigating actions taken.
- g) The NRA 2015 did not lead to the definition of exemptions in the AML/CFT framework, nor to the application of simplified or enhanced customer due diligence measures in new circumstances.
- h) The NRA 2015 was communicated to the private sector and supported the drafting of their own risk assessment.
- i) Co-operation and co-ordination between law enforcement authorities, the FIU, tax authorities and intelligence services is adequate, but the level of co-operation and co-ordination between AML/CFT supervisors, and between supervisors and the FIU is insufficient.
- j) There is a satisfactory level of co-ordination and co-operation in relation to Combating Proliferation Financing (CPF) matters.

Recommended Actions

Finland should:

- a) Ensure that there is a shared, common understanding of ML/TF risks across all relevant authorities, including through the development of an updated risk assessment.
- b) Define appropriate channels to enable AML/CFT supervisors to get relevant and timely information on ML/TF risks trends and channels
- c) Build on the NRA 2015 experience to improve the methodology used and lead to a comprehensive mapping of ML/TF risks, on the basis of which ML/TF methods can be identified and different levels of risks defined (e.g. low, medium, high etc.) to help authorities prioritise their work. The risks associated with the NPO sector and legal entities should be a full part of the analysis.
- d) Define an AML Action Plan, which should be adopted alongside the updated NRA. It should include targeted measures, both legislative and operational as required, to mitigate the risks identified. It should also define the resources required to successfully and efficiently conduct the planned activities.
- e) Enhance operational co-operation between AML/CFT supervisors, and between supervisors and the FIU, including through the work of the new AML/CFT Co-ordination Group.

111. The relevant Immediate Outcome considered and assessed in this chapter is IO.1. The Recommendations relevant for the assessment of effectiveness under this section are R.1, 2, 33 and 34.

Immediate Outcome 1 (Risk, Policy and Co-ordination)*Country's understanding of its ML/TF risks**Money Laundering Risks*

112. Finland has an adequate understanding of its economic crime risks. Finnish authorities generally demonstrated, through their activities and sets of priorities, that they have a clear representation of the national ML risk landscape. This is evidenced in particular by the national focus on combating the grey economy (see below.). The NRA 2015 only partly supports this understanding of risks as they evolve.

113. The understanding of the main ML risks, and of the ML channels, is however uneven across Finnish authorities. A number of them, including AML/CFT supervisors, have a good technical overview of the potential ML channels for their specific sectors, based on EU and international assessment guidelines. However, they do not have real experience of assessing the risks posed by institutions or sectors, nor how these individual, sectoral understanding of risks relate to the overall risk context of the country. This is of specific concern regarding the supervision of financial institutions, since such institutions play an important gateway role to the Finnish economy as a whole (see IO.3). Other agencies, including

law enforcement authorities (LEAs), have a more robust and comprehensive understanding of the risks, based on their intelligence gathering and investigative activities.

Terrorism Financing Risks

114. Key national authorities for combating TF have a sound understanding of TF risks. This is particularly the case for the FIU, the National Bureau of Investigation (NBI) and the Finnish Security Intelligence Service (SUPO). Their assessment and monitoring of the terrorism threat for the country, as well as typologies and analysis conducted on existing TF trends provide them with solid TF knowledge. Those agencies are at the forefront of the detection of potential terrorism and TF cases. In this capacity, they play a central and alert role vis-à-vis other institutions in the country (see IO.9). Supervisors' understanding of TF risks is not comprehensive enough, and this can negatively impact the implementation of relevant preventive measures by reporting entities (see IO.3).

115. While the understanding and assessment of the current TF threat is good, more focus could be given to the emerging threats and mid- to long-term developments (e.g. returning FTFs), with a view to anticipate changes and adapt the response.

National Research Report on ML/TF risks (NRA 2015)

116. Finland conducted its first research on ML/TF risks in 2014/15 (see Chapter 1, 1.1.2.). This report identified six key risk items, which constitute the national risk assessment: real estate investments, transport of cash, front companies, increasing online services, online shadow financing markets and customer fund accounts. Although some of the key risks identified remain critical for Finland's front companies and cash transport (see section below), overall the analysis and conclusions need to be reviewed to reflect the evolution of the national risk context and mitigating actions taken. An example of that is the area of real estate investments, where real estate professionals no longer accept cash payments and the economic situation has limited the ability of foreign nationals (e.g. Russians, Estonians) to buy property in Finland. Regarding customer fund accounts, legal professionals and real-estate agents avoid using them, and supervisory measures have been introduced (see IO.4).

117. The NRA 2015 identified virtual currencies as a serious ML/TF risk (as part of the "increasing online services"). It focused on their use in the gaming field although it has been confirmed that virtual currencies have been used in economic crimes and drug-related cases by organised crime groups (see Chapter 1 and the section below). Finland has initiated regulatory work on virtual currencies, and plans to present mitigating actions in autumn 2018.

118. Finnish authorities intend to conduct a new national ML/TF risk assessment in 2019/20. This is a positive step, as it will be an additional, shared means to further improve the risk's understanding of national authorities. In preparation for this work, Finland should develop and adopt a methodology which includes both qualitative and quantitative measures to facilitate the identification and assessment of current and emerging ML/TF risks. The methodology should specifically address weaknesses identified in the methodology adopted for the NRA 2015. For example,

the need to better balance the assumptions or perceptions of involved parties (e.g. assessment through online surveys) with quantitative and objective data (e.g. STRs, cross-border financial flows); to draw conclusions based on confirmed threats or vulnerabilities, and not on factors unrelated or only indirectly related to ML and TF (e.g. the geopolitical situation, growing trends at the international level etc.); to expand the dialogue and exchanges of views between interested stakeholders on the threats and vulnerabilities, and risk factors identified.

119. The general focus of the assessment should also be reconsidered, with a view to come up with a shared mapping of ML/TF risks, on the basis of which ML/TF methods can be identified. The risk assessment needs to identify both the main risks to which Finland is exposed, as well as the channels through which ML and TF materialise in the country. The NRA 2015 focused on the methods criminals use, or could potentially use, mainly to launder proceeds of crimes, and the final list of key risk items only includes means through which money is laundered in Finland. However, a complete and holistic picture is needed both to address the ML/TF risks faced by Finland, and to take the appropriate mitigation measures regarding the channels used or abused by criminals. In that regard, TF risks should be more specifically looked at, as the TF vehicles used present distinctive features.

120. Finnish authorities should adopt a global approach to turn the ML/TF risk research into a national reference framework for AML/CFT. The assessment part of the analysis should be enhanced, and different levels of risks (e.g. low/medium/high) should be defined to help Finnish authorities prioritise their work, while adopting a comprehensive approach to risks. Finnish authorities should also envisage examining the specific risks associated with Non-Profit Organisations (NPO) and legal persons and arrangements as part of their next risk assessment initiative. Finally, the risk assessment should be released together with an action plan detailing how the risks identified will be addressed and mitigated.

121. The EU supra-national risk assessment was published in June 2017,⁵⁴ and therefore its conclusions could not be taken on board in Finland's NRA 2015. However, it was used for the June 2018 AML Action Plan (see below.), which added trade in works of art as a 7th key risk item for Finland. This was also based on the NBI and FIU's reporting of serious and organised crime cases involving works of art and antiquities, which have amounted to approx. EUR 20 million since 2009.

National policies to address identified ML/TF risks

122. The 2016/2020 National Strategy on the Prevention Grey Economy and Economic Crime (see Chapter 1) sets a relevant framework to address the main ML risks identified in a coordinated manner and puts forward a preventive approach to economic crime. Fighting the grey economy and economic crime is a standing policy priority for Finland, justified by its social model, which is a key pillar of national market competitiveness (skilled labour force, strong social cohesion etc.). Over the years, including due to measures of successive national strategies and associated Action Plans, Finland has built a solid and extensive tax-based preventive framework. It has facilitated and encouraged individuals and companies' compliance with their statutory payments and obligations, including for business activities where undeclared work was a major concern, like the construction sector. The scope

⁵⁴ http://ec.europa.eu/newsroom/just/item-detail.cfm?item_id=81272

of those measures has also enabled Finland to introduce some transparency and registration obligations to cross-border workers and companies from neighbouring countries with which business relationships are most developed, such as Estonia. Open and easy access to information has successfully promoted the development of business relationships with reliable partners. Equally, the reduced burden for the fulfilment of businesses' tax-related obligations has increased the compliance rate. Those tax-related measures aim at preventing and blocking the development of grey economy activities in Finland at the earliest stage. In so doing, they also reduce the risk that proceeds of tax offences are available for ML.

123. The Strategy on the Prevention of the Grey Economy and Action Plan also promote enhanced co-operation between public authorities. In that respect, the "Compliance reports" developed by the Grey Economy Information Unit (see Chapter 1) are powerful tools to enable authorities to share information on a given person or company, and provide access to consolidated sets of information from a range of sources (tax, pension, accident insurance, customs payments etc.), through a single contact point and almost in real time. Access to this information by an increasing number of authorities - including the financial supervisor (FIN-FSA) as recently as June 2018 - is a positive development. These reports have proved useful for authorities involved in AML/CFT activities, and especially the FIU, to get background data and information on persons and organisations suspected of being involved in ML/TF cases, and on sources of suspected funds (see IO. 6).

124. The positive effects of the grey economy preventive measures have to be assessed in conjunction with the limited use of cash in Finland, and the vast majority of payments and financial transactions involving bank accounts (see Chapter 1, 1.2).⁵⁵ In addition, the use of cash is restricted, among other things by the Employment Contract Act, in order to combat the grey economy.⁵⁶ Combined with tax-related preventive measures, this creates robust safeguards to prevent illicit money and proceeds of predicate offences from entering and circulating through regulated financial channels in the country.

125. It has to be noted though, that due to the heavy tax focus of Finnish authorities, investigations and prosecutions tend to prioritise tax predicate offences over ML (see IO. 7).

126. The AML Action Plan adopted in June 2018 as part of the 2016/2020 Grey Economy Strategy is based on the NRA 2015 which does not reflect the current ML risks in the country. It also takes into account the June 2017 EU supranational risk assessment, and based on its conclusions adds trade in works of art as a 7th key risk item for Finland (see section on Country's understanding of its ML/TF risks).

127. The 2018 AML Action Plan is not ambitious enough regarding the proposed measures to tackle the risks still relevant in the current context. On cash transportation and front companies, the Action Plan mainly proposes to strengthen the implementation of existing measures or recalls planned measures or ongoing initiatives. It does not envisage any new national legislative and/or operational initiatives. It would be useful for example to set objectives and priorities in terms of cash controls to be conducted (e.g. numbers and types, target groups, priority

⁵⁵ 99,8% of the population in Finland hold a bank account, World Bank 2017 <https://globalfindex.worldbank.org/sites/globalfindex/files/countrybook/Finland.pdf>

⁵⁶ AML Action Plan, Section 4.2

borders and type-land, ports, airports etc.), including joint operations with domestic authorities or international counterparts, which are only briefly mentioned. For front companies, the only measure mentioned is the set-up of the national beneficial ownership register (by 30 June 2019), while recognising that it will not solve all identified problems (see IO.5).

128. Other major ML risks identified in Finland – drugs and frauds – are adequately addressed by Finnish authorities, based on mutually supportive actions between relevant authorities. Drug proceeds are mostly generated in cash form and smuggled out of the country via the Baltic States. Some proceeds are commingled with the legitimate income of small businesses (such as restaurants or tattoo shops) owned by criminals or their associates. There is a trend, not significant in absolute terms, but growing, that payments for illicit drugs take place using virtual currencies. The Police is working closely with the Border Guard and the Customs in combating drug crimes. Customs are developing profiles of sensitive travellers and conducting targeted searches on that basis. These profiles are regularly updated depending on the changing crime picture.

129. Another major ML threat is the proceeds generated from both domestic and foreign frauds, including tax fraud, identity theft, cybercrime, romance scams, etc. Tax frauds are often more sophisticated and involve the use of offshore structures and bank accounts set up by professional intermediaries resident in foreign jurisdictions. Significant parts of the proceeds generated by these crimes are moved outside of Finland. Other types of frauds typically involve money mules – local residents, often without stable income, who agree to let their bank accounts be used to wire the proceeds of fraud for a certain fee and then transfer the rest to the perpetrator, using either a bank account or a money remitter. Tax fraud having the largest share of all types of fraud is dealt with in the context of the Strategy on the Prevention of the Grey Economy. Other types of fraud are among the priorities of the Police and the FIU.

130. The Finnish Eastern border with Russia is also an external border with the EEA and the EU. The main risk here stems from cross-border transportation of undeclared cash, which may have illegal origins. Customs have adequate measures in place to monitor the Eastern border and, together with Police, have established good co-operation with their Russian counterparts. This involves co-operation and mutual assistance agreements in customs matters, and more general crime prevention and combatting. It also includes the presence of liaison officers (Customs, Police) in both countries (see IO.2). This has resulted in a number of investigations based on Customs operations (see example in Box 2.1), as well as in seven Customs enforcement operations between 2014 and 2018, involving customs authorities of Finland and Russia. The scope of these operations (whose details are confidential) included cash money among other targeted goods. Several inspections were conducted and declared and undeclared cash was discovered during these operations.

Box 2.1. Cargo case (see more on this case in Box 8.3 in IO.2)
Co-operation between Russian and Finland based on customs operation.

A group of Russian couriers carried over EUR 20 million from an Estonian bank to Russia via Finland during an approx. eight month period in 2011-12. The funds were sent to the Estonian bank from Russia (RUB) and returned to the sender in cash (EUR). An FIU case was opened and a freezing order was given to the Customs for a value of about EUR 3.6 million.

The Finnish National Bureau of Investigation (NBI) opened a criminal investigation into aggravated ML in 2012. Co-operation with the Russian authorities started with MLA requests.

Closer co-operation with Russian authorities started in 2016 after the Investigative Committee of the Russian Federation had initiated a criminal investigation in the autumn of 2015, regarding the activities of the owner of the funds being also under investigation by the NBI. Parallel investigations were conducted in Russia and in Finland into the crimes committed by the same persons. The investigators met several times during the criminal investigation and agreed on measures to be taken. In 2017, Russian investigators spent one week in Finland in order to interview witnesses. At the same time, the NBI received valuable evidence from the Investigative Committee in the framework of mutual legal assistance.

The criminal case in Russia is **currently** in court. Nearly 20 persons are accused of smuggling and of organised crime. The criminal investigation in Finland is in its final stage and will be transferred to the prosecutor **in 2019**. The funds are still seized in Finland.

131. There have been several cases concerning complex asset movements and links to assets originated from Russia, inter alia the “Russian laundromat” case, where payments allegedly received from Russian business partners by Finnish small and medium-sized companies were affected. These funds proved to be linked to shell companies registered in high secrecy jurisdictions. Cases linked to this scheme have been analysed by the FIU as well as the NBI, and some investigations are still ongoing, or pending a prosecutor’s decision on indictment. Even if the actual criminal situation does not show Russian-related ML as a high risk, the geographical proximity and large volumes of goods and assets flows between Finland and Russia pose a risk for involvement of criminal elements (see Chapter 1, 1.1.1). High ML/TF risk perception of businesses and client groups associated with Russia is generally based on geopolitical concerns (e.g. sanctions).

132. Finland addresses the identified TF risks in a manner which is consistent with the nature and level of TF risk in the country, which mainly originates from sympathisers of terrorist cause, as well as FTFs and returned FTFs (see Chapter 1.). TF is part of all terrorism related intelligence gathering activities and investigations, with a focus on returning FTFs. Consequently, CFT activities are based on a collaborative and information-sharing approach between all relevant authorities, irrespective of whether the potential TF case is identified through a potential terrorist target (e.g. by intelligence services) or a suspicious transaction (through a report filed with the FIU) (see IO.6 and 9).

133. Money transfer channels are flagged by relevant authorities and the private sector as vehicles carrying TF risks. Measures have been taken to encourage the registration of hawalas, but unregulated and informal money transfers remain an issue due to the costs associated with registration and the difficulty of maintaining banking relationships (see IO.3). The parts of the NPO sector at specific risk of TF abuse are subject to money collection controls, with limited TF focus (see IO.10). The 2014 counter-terrorism strategy, updated in 2016 includes a CFT aspect which focuses on NPO monitoring. The FIU recently conducted a review of STRs received between 2016 and 2018 related to NPOs but the results have not been disseminated (as they were based on confidential information), nor led to any specific initiative so far.

Exemptions, enhanced and simplified measures

134. The NRA 2015 did not lead to the definition of exemptions to the AML/CFT framework, nor to the application of simplified or enhanced customer due diligence measures in new circumstances.

135. The exemptions currently included in the AML/CFT Act are subject to relevant low risk conditions and quantitative thresholds (see TC Annex, c. 1.6).

136. The AML/CFT Act allows obliged entities to apply simplified due diligence measures (SDD) when ML/TF risks are “negligible”, on the basis of their risk assessment. A government decree will define factors indicating situations when the risks can be viewed as “negligible” (see TC Annex, c. 1.8 and 10.18). The government decree, still under consideration at the end of the on-site visit, should make clear that the negligible risk factors should only be indicative elements for obliged entities, and each obliged entity’s individual risk assessment will have to confirm the lower level of risk.

Objectives and activities of competent authorities

137. The priorities and activities of the law enforcement community, intelligence and tax authorities are aligned with the national risk landscape. The law enforcement agencies devote a considerable amount of their crime prevention and investigative resources on the most risky areas, such as tax crimes, fraud and drug trafficking. Nevertheless, for ML related to drug crime, actions towards organised crime should intensify, and not only target the predicate offence (see IO.7). TF is part of the 2014 National Counter-Terrorism Strategy and its June 2016 update. Accordingly, TF is one of the highest priorities for SUPO and the FIU (see IO.9).

138. Supervisors’ ML/TF risk-driven objectives and activities are limited. In general, supervisors’ understanding of risks is still fragmentary (see section 2.2.1). ML/TF risks are an important priority for supervisory authorities at this stage, since most of them are in the process of conducting risk mapping and profiling of the different sectors and obliged entities under their supervision, in order to define the methodology and tools which will enable them to conduct risk-based supervision.

139. Nevertheless, both FIN-FSA, the financial supervisor, and the RSAA, responsible for the supervision of some non-banking financial institutions and some DNFBPs, such as accountants or real estate agents (see Chapter 1, Table 1.2), have focused their supervisory activities, including inspections, on sectors perceived as higher risk. This means that the AML/CFT supervisory focus so far has been on the

banking sector, and in particular the largest banks, and also, but to a lesser extent on registered hawalas, as well as on real estate agents (see IO.3).

National co-ordination and co-operation

140. Co-operation and co-ordination between law enforcement authorities, the FIU, tax authorities and SUPO is adequate. There are established channels of communication between these authorities and they often make use of joint investigative teams depending on the subject and complexity of the case. A number of examples were given, including of joint investigations between NBI and Customs in ML cases related to drug trafficking, or in intelligence-sharing for TF cases (see IO.7 and 9).

141. The level of co-operation and co-ordination between AML/CFT supervisors is not sufficient. There are occasional, case-by-case exchanges of information between supervisors, mainly between FIN-FSA and RSAA. However, there would be benefits to expanding co-operation between all AML/CFT supervisors, with a view to increase the convergence of supervisory practices. Sharing of experiences, good practices and tools to improve the approach to AML/CFT supervision on a risk-basis would also be of value.

142. Co-operation between the FIU and supervisors is uneven: while FIN-FSA receives targeted information when appropriate (e.g. biennial reports on STRs received from supervised entities, strategic analysis of higher risk areas), communication is more limited with other supervisory bodies. It would be useful for all supervisors to have better and more frequent dialogue with the FIU, especially to get a better understanding of the risks - TF risks and typologies, and emerging ML/TF trends in particular-, and develop joint work to improve STR reporting by supervised entities. It is noted that the authorities have established the AML/CFT National Co-ordination Group in May 2018, with a view to enhance and improve operational co-ordination and co-operation between the FIU, supervisors and law enforcement agencies.

143. There is a satisfactory level of co-ordination and co-operation in relation to combating proliferation financing (CPF) matters. The Ministry of Foreign Affairs (MFA) as the main authority for PF-related issues, works in close co-operation with other involved parties such as the export control authority for dual-use items (also within the MFA) and law enforcement authorities. There is also good co-ordination, as well as intelligence and information-sharing, with SUPO and Customs. The Sanctions co-ordination Working Group, also chaired by the MFA is the main forum for co-operation and co-ordination between authorities having a role in the enforcement of PF TFS (FIN-FSA, Immigration Services, Customs, SUPO, Ministry of Justice, Ministry of Interior etc.), and meets on a yearly basis.

Private sector's awareness of risks

144. Private sector representatives were aware of the results of the NRA 2015. The outcome of this report was broadly communicated in Finland, through TV, radio and social media. The final document is available on the FIU's website.⁵⁷ However, mixed views were expressed with regard to the continued relevance of the

⁵⁷ www.polamk.fi/tki/projektihaku/raterisk

information included and the key risk items list. A number of financial institutions and DNFBPs indicated that the report was too general to be of direct relevance for their own risk assessments.

145. In general, financial institutions are well aware of their ML/TF risks, with a more developed understanding among larger financial institutions and those belonging to international groups, as they can benefit from their groups' experience and knowledge. As far as DNFBPs are concerned, casino operators have a practical understanding of ML/TF risks they face. There is a lesser level of risk understanding amongst real estate agents, lawyers and accountants, and dealers in precious metals and stones (see IO.4).

Overall conclusion on IO.1

146. **Finland has achieved a substantial level of effectiveness for IO.1.**

CHAPTER 3. LEGAL SYSTEM AND OPERATIONAL ISSUES

Key Findings and Recommended Actions

Key Findings

Use of Financial Intelligence (Immediate Outcome 6)

- a) Financial intelligence along with other relevant information is used to a high extent in investigations to develop evidence and trace criminal proceeds related to ML and associated predicate offences. Financial intelligence plays an important role in the CFT domain as well.
- b) There is a wide range of different reports (STRs, cross-border currency reports, etc.) available to competent authorities, with most of them containing accurate and relevant information. The authorities actively request and receive these reports in order to perform their duties. An important source of financial intelligence is Compliance Reports produced by the Grey Economy Information Unit (GEIU) within the Tax Administration.
- c) The FIU analysis and dissemination supports the operational needs of the competent authorities to a moderate extent. The FIU analysis and dissemination contribute both to starting new criminal investigations and to supporting ongoing cases, although the overall number of ML cases using intelligence products of the FIU is modest. The FIU produces quality strategic analysis. However, its use by other competent authorities is limited.
- d) The FIU has established good co-operation with law enforcement authorities and the Tax Administration, which enables it to exchange information and financial intelligence in a secure manner. However, co-operation with the supervisors has been limited and has not yielded concrete results.
- e) The FIU is actively engaging with its foreign counterparts using secure channels of communication.

ML Investigation and Prosecution (Immediate Outcome 7)

- a) ML cases are identified through the active involvement and intelligence gathering of all relevant authorities, including the FIU, Customs and tax authorities.
- b) Authorities most often investigate ML offences as an integrated part of the criminal investigation of the predicate offence (“follow the money” approach). This has a limiting effect on the number of investigations of stand-alone ML offences.
- c) Law enforcement authorities conduct complex and international investigations involving foreign predicate offences and significant amounts of laundered proceeds, and are able to mobilize joint investigative teams and use advanced investigative tools. Finnish investigators have appropriate skills and experience. Nevertheless, the

opening of criminal investigations could be contained by a restrictive approach to the opening conditions.

- d) ML investigations and prosecutions are consistent with the country's risk profile in particular with regard to grey economy-related offences. Drug trafficking cases focus on individual dealers rather than on organised crime groups.
- e) Cases are brought to courts by the prosecution service to a satisfactory extent. They lead to convictions in 70% of the cases, which is consistent with the average ratio in other criminal cases.
- f) However, the rule of concurrent offences (i.e. the most serious crime is prosecuted when several offences have been committed) makes it difficult to get an overall picture of ML convictions by Finnish courts. There have only been a few prosecutions and no convictions of self-laundering in aggravated ML. The concurrency rule can also impact the decision to prosecute ML separately from the predicate offence and therefore possibly contains the number of standalone ML investigations.
- g) Penalties for ML offences are not fully proportional as cumulative fines may be ordered only in conjunction with conditional imprisonment but not in conjunction with unconditional imprisonment. Courts do not use the full range of penalties available and sentencing practice is lenient.
- h) Authorities do use other approaches to combat ML, especially by pursuing other financial crimes. However, they do so because of other policy priorities and objectives such as combating tax crime, even though it would be possible to pursue the ML offences. This approach constitutes a substitute for ML investigations, and limits the importance of ML prosecutions and convictions.

Confiscation (Immediate Outcome 8)

- a) Finland pursues confiscation as a policy objective and has developed a far-reaching legal framework to recover assets, including mechanisms to facilitate decisions to confiscate.
- b) Provisional measures are available. At the early stage of the process, significant amounts are frozen by the FIU. Seizures measures are in place at the criminal investigation stage, which are routinely used by the relevant authorities.
- c) Seized amounts are compensated to the victims as a matter of priority in Finland, over confiscation to the state. Therefore, the confiscation decisions, and the amounts involved, do not fully reflect the extent to which criminals are deprived of their assets.
- d) Finnish authorities, despite their high-level engagement and legislative improvements, lack comprehensive statistics to demonstrate and assess whether the policies are actually successful in permanently depriving criminals of their assets. In any case, confiscations in cross-border ML cases and repatriation of assets to Finland are insignificant.
- e) There are some indicators that measures taken to deprive criminals of their assets are aligned with the major ML risks of Finland but it is not confirmed that it translates into permanent confiscations or compensation.

- f) Confiscation in cross-border cash transportation cases is not applied to a satisfactory extent.
- g) As regards deprivation of assets related to TF, it is not fully in line with the country's risk profile as only limited steps have been taken to freeze assets of FTFs.

Recommended Actions

Immediate Outcome 6

Finland should:

- a) Encourage law enforcement authorities (especially local police departments) to engage more actively with the FIU to leverage its potential of producing quality financial intelligence
- b) Consider increasing the FIU's resources devoted to analysis of STRs, or otherwise improve its working processes, as it may face a shortage of human resources in view of the constantly growing numbers of STRs and their manual processing.
- c) Urge competent authorities, especially supervisors, to make more active use of the strategic analysis produced by the FIU, and to enhance their co-operation, including through the newly set up AML/CFT Co-ordination Group.

Immediate Outcome 7

Finland should:

- a) Allow for self-laundering convictions for non-aggravated ML offences and for convictions where the ML offence does not prevail over the predicate offence.
- b) Increase LEAs' focus on ML investigations and prosecution, in particular through the promotion of a more proactive approach to opening ML cases.
- c) Develop statistics at the court and prosecution level with a view to increasing awareness of the conversion rate of ML investigations into ML prosecutions, as well as about the number of convictions and sentencing practices for ML cases.
- d) Encourage the use of a wider range of sentences for aggravated ML cases by courts, to improve the proportionality of sentencing.

Immediate Outcome 8

Finland should:

- a) Urge relevant authorities to finalise a concrete plan of action to trace, safeguard and confiscate the proceeds of crime, as part of the ongoing project conducted in the context of the 2016/20 Action Plan against Shadow Economy and Economic Crime.
- b) Address the limitations that affect mechanisms in place to facilitate the recovery of assets, with a view to extend their scope to the full range of ML-related offences.
- c) Provide comprehensive statistical support on confiscation and related

- measures to deprive ML/TF criminals of proceeds, as a mean to measure and improve the effectiveness of its AML/CFT policies and related actions.
- d) Develop legislative measures and mechanisms to confiscate cross-border movements of currency that are falsely or not declared, as an effective, proportionate and dissuasive sanction.
 - e) Support actions to enhance asset freezing measures applied to FTFs.

147. The relevant Immediate Outcomes considered and assessed in this chapter are IO.6-8. The Recommendations relevant for the assessment of effectiveness under this section are R.1, R. 3, R.4 and R.29-32.

Immediate Outcome 6 (Financial Intelligence ML/TF)

Use of financial intelligence and other information

148. Financial intelligence along with other relevant information is used to a high extent in investigations to develop evidence and trace criminal proceeds related to ML and associated predicate offences. Financial intelligence appears to play an important role in CFT domain as well.

149. Proceeds of crime are traced as a matter of policy and financial intelligence is routinely utilised for that purpose. There is a number of sources of quality financial intelligence, such as FIU analysis, information obtained from FIs and DNFBPs reports on cross-border transportation of currency, compliance reports compiled by the Tax Administration database, as well as law enforcement intelligence, the criminal investigations database. Multiple state registries on population, business and property further complement this information.

150. Collecting and requesting financial intelligence is daily work for police investigative units in financial crime investigations and in other cases where proceeds of crime are involved. In addition to financial intelligence produced by the FIU, all police units have their own mechanisms (which do not require a court order) to collect financial intelligence from FIs and DNFBPs for the cases they investigate. Using financial intelligence for developing evidence of ML is especially widely used in tax fraud cases (which represent the vast majority of ML cases, see IO.7). These are often real-time investigations, in which evidence on the proceeds of crime is collected while the criminal activity is still ongoing. Financial intelligence is also used to establish connections and map criminal networks.

151. There is no precise estimate on the share of cases where financial intelligence was used to trace proceeds of crime or develop evidence of ML. However, the assessment team is convinced that it is done in almost every relevant case. On average, the Finnish police, as part of its investigations, made around 2 300 requests to four of the five biggest banks per month for banking information/financial intelligence during 2017. It also started the project of electronic banking requests in April 2017, although the results will be operationalised in 2019. As mentioned above, using financial intelligence is a matter of policy in the financial investigations. It is one of the internal indicators of performance for the investigative units, and it is followed closely at the management level.

152. Financial intelligence appears to play an important role in the CFT domain as well. Although it is hard to judge its usefulness based solely on a single case in 2016, close co-operation between the FIU and the Finnish Security Intelligence Service (SUPO) in the intelligence gathering stage seems to be a positive indicator (see section below, for example).

153. An important source of financial intelligence is the Grey Economy Information Unit (GEIU) within the Tax Administration, which produces so-called “compliance reports” (see Chapter 1). Their main objective is to support operational actions against the grey economy, which includes, *inter alia*, economic crime investigations. The NBI and the Customs regularly access and use the compliance reports to investigate tax frauds, narcotics offences as well as to trace criminal proceeds, and obtain a comprehensive picture about the business activity of the company involved in the suspected crime. Although there is no information available about the share of the compliance reports used in those investigations, the authorities consider them valuable.

154. The GEIU and the FIU together have built up an automated mechanism to import the Compliance reports of all the companies in the FIU database automatically once a day. Since May 2018, all cases analysed by the FIU have included information from Compliance reports.

Reports received and requested by competent authorities

155. There is a wide range of different reports available to competent authorities, with most of them containing accurate and relevant information. The authorities actively request and receive these reports in order to perform their duties.

156. The reports are mainly collected by the FIU, Customs and Tax Administration (see Table 3.1 below).

Table 3.1. Reports received/produced by the competent authorities

	2015	2016	2017
STRs by the private sector	5 190	6 096	8 090
Threshold reports	32 400	24 773	39 960
Suspicious reports by Finnish public authorities	70	111	110
Cross-border cash declarations over EUR 10 000	294	283	244
Compliance reports	161270	192613	275000

Source: Finnish authorities

157. *STRs* - STRs are the main source of financial intelligence. The quality of STRs can vary, with the bigger banks providing higher quality reports, i.e. containing relevant and accurate information. However, the STRs submitted by smaller reporting entities are of less value. Most of the STRs (around 99%) are submitted electronically through a web application (GoAML). It contains a pull down list of 34 indicators from which the reporting entity can choose one or more reasons to submit an STR, such as ‘unusual account transaction(s)’, ‘origin of assets unknown’, ‘unusual cash deposit’, etc. The purpose of the list is: a) to assist reporting entities to indicate their reason(s) for submitting STRs and b) to assist the FIU to identify increasing/decreasing ML or TF avenues. The quality of reports related to TF is generally lower, as the abilities of the reporting entities to identify potential TF-

related targets are limited. The FIU instructed reporting entities that it is more important to file a report than to worry about the type of the report. That does not appear to be a major problem, since the FIU makes an independent evaluation of a STR in every case, and subsequently re-qualifies it as appropriate.

3

158. Only FIU staff has access to the STRs database. However, law enforcement authorities (LEAs) may obtain that information on request. Although the FIU has recommended that LEAs file requests to obtain access to STR information, this is not a regular practice (see Table 3.2). More information on the analysis and use of STRs is given in the subsequent section. The FIU, to a large extent, also spontaneously disseminates the information to ongoing investigations (see Table 3.6).

159. *Threshold reports* - In addition to STRs, reporting entities are submitting reports that are based on a combination of objective risk factors, established internally by institutions themselves. These factors also include the value of transactions. For each institution, these factors (and value thresholds, accordingly) may be different depending on their risk profile. Since 3 July 2017, money transfer service providers are obliged to submit threshold reports for transactions over 1 000 EUR. This obligation does not rely on a formal risk assessment but rather on the presumption of the risk level set in the AML/CFT law and the perception that compliance resources available to these entities are insufficient⁵⁸. The gambling operators have also modified similar internal criteria for reporting (undisclosed to the assessment team), following recommendations from the FIU to increase quality of reporting. These reports outnumber the STRs. They are not analysed individually as a matter of course, but they serve as an additional source of information when building a case by FIU analysts.

160. Similar to STRs, only the FIU has direct access to threshold reports, however they are available to other competent authorities on request.

161. Table 3.2 shows the requests from domestic law enforcement authorities for information held by the FIU. This includes information contained in the STRs and threshold reports.

⁵⁸ Legally all reports received by the FIU are considered STR reports (including the threshold reports).

Table 3.2. Requests from domestic LEAs

Requesting Authority	2015	2016	2017
NBI	71	47	46
Helsinki Police Department	33	27	26
Other regional police departments	28	38	37
SUPO	16	7	3
Customs	2	12	11
Border Guard	2	8	6
Tax Administration	1	1	0
Other	0	2	0
Total	153	142	129

Source: FIU

162. *Cross-border cash movements reports* - Customs collects reports on cross-border cash declarations over EUR 10 000 entering or leaving EEA. This information is received by the FIU on a monthly basis and automatically matched against the FIU database subjects. These reports serve as an additional source of information when building a case by FIU analysts. Cross-border cash declarations are also available to all police, border guard and customs units.

163. There are no detailed statistics on the use of cross-border cash reports by the competent authorities. However, by matching against information in the declarations, the FIU was able to identify 250 persons as potential cash couriers who were linked to suspicious transaction reports on themes such as: cash from the Middle East, cash connected to hawalas, reports of large cash deposits to accounts, money transfer information, tax fraud suspicions, gambling, as well as open criminal investigations. Between August 2016 and May 2018, based on this analysis the FIU made 44 disseminations to the competent authorities (SUPO, Customs) concerning individuals identified as cash couriers.

164. *Reports by public authorities* - Customs, the Border Guard, the Tax Administration, the Supervisory Authorities, the Office of Bankruptcy Ombudsman and the Enforcement Authorities have an obligation to report suspicions of ML or TF to the FIU, if they come across potential cases in the course of performance of their duties. Although not as numerous as other types of reports, they represent an important source of financial intelligence. These reports are produced by competent authorities who have a good level of awareness of ML/TF issues, and therefore the information contained in them is of high quality (see Table 3.3). For example, around 75% of the reports submitted by the Enforcement Authorities led to further analysis and around 40 % to further investigations. There is no information available on the use of these reports by other authorities.

Table 3.3. Suspicious reports by the public authorities

	2015	2016	2017
Total	62	109	94
Enforcement Authorities	12	14	36
Tax Administration	13	24	32
Customs	34	71	19
Other authorities	3	0	7

Source : FIU

165. *Compliance reports* - Compliance reports produced by the Grey Economy Information Unit (GEIU) of the Tax Administration are another important source of financial intelligence information on economic crimes related to tax fraud (see Chapter 1, 1.2.1). The demand for these reports is growing which is evidence of their utility for the competent authorities, see Table 3.4.

Table 3.4. Requests for Compliance reports

	2015	2016	2017
Total	161 270	192 613	275 000
Police, including the FIU	3 462	5 968	4 913
Customs	n/a	641	2161

Source: Finnish authorities

166. *Requests for information to private sector* - The FIU and the NBI have the statutory power to request any information from any entity in Finland deemed necessary to carry out their analytical functions and investigations (see TC Annex, R. 29 and 31). This request can be based on an ongoing FIU analysis or a criminal case, a request by foreign counterparts or a domestic request. The right to obtain information covers all documents and information held by the entity related to the requested customer or transaction. This includes CDD data, transactions data, and all documents attached to the obliged entities' customer and transaction files. The FIU regularly uses their power (456 requests in 2015, 381 in 2016 and 357 in 2017). Statistics on NBI requests are not available.

Operational needs supported by FIU analysis and dissemination

167. The FIU analysis and dissemination supports the operational needs of the competent authorities to a moderate extent. The Finnish FIU is a police-type FIU, located within the Police (National Bureau of Investigation, NBI). It is one of the sources of financial intelligence for law enforcement and other competent authorities. The FIU has unique capabilities to establish complex connections and patterns between persons, assets and activities. The FIU analysis and dissemination contribute both to starting new criminal investigations and to supporting ongoing cases, however the overall number of ML cases using intelligence products of the FIU is modest. The FIU produces quality strategic analysis, however its use by other competent authorities is limited.

Operational analysis

168. Every STR entering the FIU database is analysed. At the first stage, a STR is automatically enhanced with information from other databases that the FIU has online access to if there is any match between the data fields of the STR and entries in those databases. The FIU uses GoAML software system in its work. The FIU has direct access to an extensive range of useful and relevant registers, such as: Population Information System (family, address information); Company Register; Vehicle and Watercraft Registers; driving licences; Passport Register (Finnish passports); border crossings of persons entering Finland with a visa; Visas granted by Finland to foreign nationalities; Land Information System; – Register of Aliens by Finnish Immigration Service; Criminal Investigation Database (Police, Customs, Border Guard); Criminal intelligence database (Police, Border Guard); Schengen Information System (SIS II); Europol SIENA and EIS; Interpol I24/7; Database on International Information Exchange (i.e. incoming/outgoing requests). In addition, the IT system of the FIU performs automatic requests to the GEIU database to identify matches of the subjects of an STR with its Compliance reports. The result of the request further enhances the STR.

169. At the next stage, one of 20 FIU experts conducts a preliminary analysis of this “enhanced” STR with the main purpose of identifying cases in which there is a link between the subjects or transactions mentioned in the report and criminal or potential criminal activity. After the preliminary analysis, the analyst makes a decision on whether the report should be archived (i.e. no further action is taken) or escalated to a Case Proposal (CAP). The Case Proposals are sent to the FIU Commanding Officer to be evaluated and prioritized, and possibly to be escalated to a Case (CAS). There are formal criteria for prioritising cases, which seem to be broadly in line with the ML/TF risk profile (from highest to lowest):

1. Terrorist financing cases and related international projects: ISIL 3 (led by the Egmont Group), ISIL (led by the FATF)
2. Freezing and possible confiscation of criminal assets
3. New criminal investigation - ongoing crime
4. Criminal cases related to serious organised crime
5. Co-operation cases with economic crime intelligence
6. International AML and economic crime projects: EMPACT, XBD⁵⁹
7. Fraud, embezzlement (when there are no freezing possibilities)
8. Complex cases (no resources for long term analysis and investigation)
9. Threshold Reports; suspicious cash/ATM behaviour
10. Gambling cases with significant losses

170. After a case has been opened, a case analyst conducts a more thorough analysis. In addition to the tools available directly to the FIU (direct access to databases / information), the necessary additional information is obtained by sending requests domestically or to foreign counterparts. The FIU has broad powers to obtain information from any private or public entity in Finland. Due to its enhanced IT system, the FIU has unique capabilities of establishing complex connections and patterns between persons, assets and activities. Once the full

⁵⁹ EMPACT: European Multidisciplinary Platform against Criminal Threats ; XBD: Cross Border Dissemination

picture of the underlying activities has been established, the Commanding Officer decides whether the case should be disseminated and to which authority.

171. Analysis of TF-related cases follows the same approach, but with closer co-operation with the SUPO. The FIU relies on the list of potential targets provided by the SUPO, as well as ongoing communication via two SUPO liaison officers working at the NBI premises (FIU being part of the NBI, see Chapter 1).

172. The average handling time of an STR is between 5 to 10 working days, which appears adequate. However, the recent trend suggests this is increasing, which may indicate potential resource constraints in future, especially as the number of reports is growing. The figures related to the analytical chain of the FIU are presented in Table 3.5.

Table 3.5. Cases processed by the FIU

	2015	2016	2017
Opened case (CAS)	666	1238	1406
Disseminated	497	1023	1283

Source: FIU

173. Where information is disseminated, there are three options:

- the FIU opens a new criminal investigation,
- information is disseminated to an ongoing criminal investigation, or
- information is disseminated for the purpose of preventing or detecting criminal activity.

174. The breakdown of the types of disseminations and their recipients are shown in Tables 3.6 and 3.7. The total numbers might not match as the same dissemination can go to different recipients simultaneously.

Table 3.6. Types of disseminations

	2015	2016	2017	Total
New criminal investigation	27	56	42	125
Ongoing criminal investigation	207	320	321	848
Prevention and detection	263	647	920	1 830

Table 3.7. Disseminations per recipient

	2015	2016	2017	Total
Police Units	347	606	403	1 356
Tax Administration	119	410	650	1 179
Customs	10	32	30	72
Boarder Guard	3	8	12	23
Intelligence Service	17	48	56	121

Sources: FIU

175. The FIU opened 125 new criminal investigations in 2015-2017. These are then investigated by district level police or by the NBI. Most of them relate to stand-alone ML, fraud (including tax fraud), grey economy-related offending (forgery, accounting offence, offences by a debtor, business prohibition, registration offence),

and embezzlement. This picture appears to be in line with the Finnish ML risk profile. Around 30% of the investigations opened by the FIU were subsequently closed by the investigating police departments, the most prevalent reason being the absence of a crime. The remaining 70% were forwarded to prosecution, which appears to be a substantial share.

Box 3.2. Case example of an investigation opened by the FIU

In August 2014, the FIU received a STR involving a money remittance agent. It appeared that the agent had first worked for one remittance service provider and then for another. In both roles, he was suspected to have committed aggravated ML. The FIU subsequently registered a new criminal case in the criminal investigation database and engaged in close co-operation with the investigating police.

Following the investigation, the matter was heard at the District Court in June 2015. The defendant was found guilty of aggravated ML.

176. The FIU contributed to 848 ongoing investigations in 2015-2017. The majority of the cases where FIU intelligence was disseminated were fraud and tax fraud, stand-alone ML, dishonesty by debtor, embezzlement and narcotics cases. Typically, information was disseminated as a package, that the investigating unit could use as evidence. The main recipients of the disseminations were the district police departments, NBI and Customs. The NBI and Customs attach significant value to the disseminations from the FIU. For example, Customs used FIU disseminations in all of its ML investigations in 2015-2017.

Table 3.8. Disseminations to ongoing investigations per recipient

	2015	2016	2017	Total
Helsinki Police Department	57	91	79	227
Other local police departments	137	192	172	501
NBI	27	57	88	172
Customs	5	17	12	34
Boarder Guard	1	6	6	13
Total	17	48	56	947

Source: Finnish authorities

Box 3.3. Case example of FIU contributing to an investigation

The police department responsible for the criminal investigation of a fraud case contacted the FIU. As a result of a CEO fraud attack on a large Finnish company, a transaction of EUR 450 000 was made from the company account to a bank account in Bulgaria on the previous day. An FIU request was immediately sent to FIU Bulgaria and a phone call was made after the request was sent. As a result, FIU Bulgaria was quick enough to freeze the bank account in Bulgaria. No transactions out of the account had been made and the total of the lost money was returned to the victim.

177. Most of the cases disseminated were related to the prevention or detection of the criminal activity. That means that the FIU did not have enough information to decide to open an investigation on its own, and therefore decided to submit the case to a competent authority for follow-up (including opening a new investigation). The main recipient of such cases was the Tax Administration, which received 1 179 cases in 2015-2017 (i.e. all of the disseminations to the Tax Administration were of that type). Out of that number, 214 cases were not taken forward (around 18%), while for the rest the Tax Administration took some actions (such as ordering tax audits), including requesting the opening of a criminal investigation in 31 instances. The main recipients of the rest of the disseminations for prevention purposes have been the NBI and SUPO. As for the NBI, disseminations have been made, e.g. to the Organised Crime Team and Human Trafficking/Illegal Immigration Intelligence Function to be utilized in their analysis. There were at least two cases when FIU disseminations to SUPO on the basis of STRs submitted by banks led to SUPO identifying persons not yet known by the agency.⁶⁰ Customs has also indicated in one of its large scale tax fraud investigations that the financial intelligence received from FIU was the starting point for the case.

Box 3.4. Case example of FIU dissemination for the purposes of prevention

An STR report was received in March 2013; the customer of the bank had suspicious transactions on her account. Large (over EUR 1.7 million, in and out) flow of assets in 2012. It was found out that the lady worked in the procurement department of a small Finnish subsidiary company of a worldwide insurance company.

The FIU contacted the Managing Director of the Finnish company and a freezing order on the account of the lady was given by the FIU. The FIU filed a criminal investigation report and the Helsinki Police was contacted and the lady was apprehended by the police. Approximately EUR 20 000 were frozen and later seized by the police.

The lady had become addicted to gambling. She was the only employee at her office with the right of use, not only the account of the Finnish company but also the parent company.

During the years she had given to her two children some thousands of EUR and the children were charged for money laundering offence.

178. Overall, the share of financial intelligence produced by the FIU and used in ML investigations varied significantly in the recent years. Looking at cases of aggravated ML (which are the most relevant cases, given that the threshold for aggravated ML is around EUR 13 000, see IO.7), the proportion of cases using financial intelligence rose from 20 to 40% in 2015-2016, but dropped to only about 15% of the cases in 2017 (see Table 3.9). This indicates that financial intelligence produced by the FIU is not used to its full potential by investigative authorities. One of the explanations for that might be that officers in the local police departments are not well aware of the work of the FIU. In addition, the capacity of the FIU to produce

⁶⁰ FIU Annual Report 2016

high quality analysis based on financial intelligence is hampered because of constantly growing numbers of STRs. There is no additional resources allocated to FIU despite of constantly increasing workload.

Table 3.9. ML and TF investigations and the role of FIU disseminations

	2015		2016		2017	
	Total	Using FIU	Total	Using FIU	Total	Using FIU
ML investigations	187	27	403	71	446	34
Aggravated	79	16	131	55	163	24
Non-aggravated	91	11	256	16	216	10
Other	17	4	16	2	21	0
TF investigations	0	0	1	1	0	0

Source: FIU

Strategic analysis

179. The FIU has carried out more than 30 strategic analysis projects. They were related to general ML trends in Finland, particular typologies (e.g., mass-marketing fraud, misuse of payment cards and remittance), threat assessments in specific sectors (hawala, NPOs, virtual currencies, legal professionals) or geographic areas (transactions to the Middle East crisis area), as well as analysis of the FIU's own performance. The FIU also produces public annual reports. Until recently, the FIU was not able to share the analysis widely due to data protection/secretcy laws, but this has recently changed.

180. The main purpose of the strategic analysis is to identify and react to trends and patterns, to have a current situation picture of the workload and performance of the FIU, to allocate resources and to support the decision making of the Head of FIU. The analysis has led to improvements in the working processes of the FIU, such as streamlining the case management system.

181. Recently the FIU has started to provide the results of the strategic analysis to the supervisory authorities. A good example of outreach to the main financial supervisor, FIN-FSA, is the study on hawalas in Finland, which describes various business models, opportunities for their misuse, as well as the observed criminal trends. The FIU also provided the FIN-FSA with bi-annual reports on STRs received from supervised entities. However, the FIN-FSA could not demonstrate how it used those reports in practice. There was no strategic outreach to other competent authorities, although the FIU is looking to develop a more proactive approach.

182. Results of another strategic analysis project on potential misuse of development aid funding for TF purposes were provided to the Ministry of Foreign Affairs (MFA), where it was used for general awareness raising.

183. The FIU also uses strategic analysis for the purposes of giving feedback to the reporting entities. This includes feedback on the overall quality and use of STRs filed, providing indicators for potential TF-related transactions, typologies on new crime phenomena, as well as awareness raising events (seminars, training sessions, bi-lateral meetings). However, only the main obliged entities (i.e. the four biggest banks) receive regular feedback from the FIU, while most institutions would welcome increased feedback from the FIU on the quality of STRs and typologies.

Co-operation and exchange of information

184. The FIU has established good co-operation with all law enforcement authorities and the Tax Administration, which enables it to exchange information and financial intelligence in a secure manner. However, the co-operation with the supervisors has been limited and has not yielded concrete results. The FIU is actively engaging with its foreign counterparts using secure channels of communication.

Domestic

185. *NBI and the police* - The FIU has very close co-operation with the NBI. The FIU is organisationally part of the NBI, and is physically located at the NBI premises, although the FIU maintains operational independence from the NBI. The FIU and the NBI have ongoing day-to-day co-operation on operational and strategic matters. There is effective two-way exchange of information between the NBI and the FIU through secure police communication channels. Annually one or two persons from the FIU are seconded part time to other NBI departments on an as-needed basis, especially when working on significant cases related to ML or predicate offences. The NBI is one of the main recipients of the FIU disseminations (see Table 3.8).

186. Regarding the co-operation with the local police units, although the FIU disseminates numerous cases, the bi-lateral co-operation could be further developed as some police officers are not well aware of the work of the FIU and therefore are not using it to its full potential. This fact might explain the modest overall share of ML investigations where financial intelligence was used (see section on the Use of Financial Intelligence and other information above).

187. *Tax Administration* - The FIU and Tax Administration maintain close co-operation on operational matters. Since February 2017, the Tax Administration has four tax auditors dedicated for co-operation with the FIU, and there are weekly meetings to discuss potential cases. The Tax Administration is both one of the main recipients of the FIU disseminations, and an active supplier of supporting information to the FIU (see Tables 3.7 and 3.9). The exchange of information occurs through encrypted email channels and automated downloads.

188. *SUPO* - The Counter Terrorism Financing Team of the FIU works closely with SUPO. Since 2016, SUPO has shared with the NBI and the FIU relevant intelligence information on persons, who are special targets in prevention of terrorism. The FIU uses this information in the analysis of TF cases. The FIU works closely with SUPO on a case-by-case basis, including having joint meetings. SUPO receives regular disseminations from the FIU using encrypted email channels.

189. *Customs* - There is good co-operation with Customs on operational matters. That concerns not only cross-border cash declarations and FIU disseminations, but also cases when the FIU orders seizures of cash discovered during customs clearance (see IO.8). In 2015-2018, the FIU took part in national and international cash monitoring and other operations organised by Customs. These operations primarily aimed to detect both incoming and outgoing remittances involving money of illegal origin, and to launch a criminal investigation into suspected ML cases. Experts from the FIU also visited Customs to give AML/CFT training. There were also exchanges

of personnel between the FIU and Customs' Analysis Unit in order to improve co-operation and understanding of each other's work⁶¹.

190. *Supervisors* - The FIU's co-operation with the supervisors has been limited. While FIN-FSA receives targeted information when appropriate (e.g. bi-annual reports on STRs received from supervised entities, strategic analysis of higher risk areas - see section on Operational needs supported by FIU analysis and dissemination above) co-operation is almost non-existent with other supervisory bodies. Although the FIU has disseminated some of its analysis reports also to other supervisors, no practical results could be demonstrated. There is a new AML/CFT Co-ordination Group established for that purpose (see IO.1). However its creation is too recent to judge its effectiveness yet.

International

191. The FIU has independent power to exchange and disseminate information with international counterparts. These include FIUs and other competent units responsible for AML/CFT prevention, detection and investigation regardless of their organisational position/location and regardless of their status. The FIU has signed a number of MoUs with its counterparts in third countries for the purposes of AML/CFT co-operation (see TC Annex, R. 29 and 40).

192. The FIU frequently seeks international co-operation from its counterparts and other authorities, to support its work. The FIU uses the information received from abroad to support and enrich its operational and tactical analysis and build connections with ongoing ML/TF cases, or to initiate ML/TF cases. The FIU also provides relevant information to its international counterparts and competent authorities, mainly on request. The FIU also spontaneously disseminates information to foreign FIUs, and other competent authorities, but in a more limited way (see IO.2 for examples).

193. The FIU uses secure communication channels to exchange information internationally, such as FIU.net or the Egmont Secure Web, but also, with certain counterparts, Europol SIENA or Interpol I 24/7.

Overall conclusions on IO.6

194. **Finland has achieved a substantial level of effectiveness for IO.6.**

Immediate Outcome 7 (ML investigation and prosecution)

ML identification and investigation

195. There are a number of authorities in charge of investigating ML activity. The Police, including local police departments and the National Bureau of Investigation (NBI), is the authority in charge of investigating ML and associated offences. The Customs and the Border Guard are also involved in investigations, but with investigative powers limited to certain types of criminal offences. There is a high-level of co-ordination between investigative and intelligence authorities involved in

⁶¹ FIU Annual Report 2016

ML investigations even though the bi-lateral co-operation between the FIU and the local police could be further developed.

196. Investigators use financial intelligence to a high extent, as an input into ML and predicate crime identification and investigations and to trace assets (see IO.6). Out of the 229 new criminal investigations initiated by the FIU between 2012 and 2017, 162 (approximately 70%) were forwarded to the Prosecution Service. For the 30% that were discontinued, in almost half of those cases (45%) no crime was found during investigation. The NBI also starts a number of investigations based on its own information.

197. Tax Authorities and Customs also identify ML cases, based on offences connected to their fields of responsibilities. For example, Customs disseminates useful information on cross border cash controls to the FIU that contributes to the identification and/or opening of ML cases. Customs has developed a yearly updated and risk-based approach for targeted cross-border cash controls, based on intelligence and trends in cash declarations of previous years concerning risky traveling routes and profiles of passengers. Customs disseminates results of these controls with the names of involved people on a monthly basis to the FIU. The FIU uses this hit list to link people to cases already under analysis. Out of the 800 names on the list since 2015, the FIU made links with 250 names in its own database. In total, between August 2016 and May 2018, 44 such disseminations have been made concerning individuals identified as cash couriers.

198. Authorities most often investigate ML as an integrated part of the criminal investigation of the suspected predicate offence. Finnish investigators (and prosecutors) have a “follow the money” attitude in their investigative strategies, based on the obligation of the Criminal Investigations Act. Therefore, there is an integrated ML investigation within the investigation of predicate offences, as opposed to a parallel ML investigation. LEAs’ priorities are to prosecute offences that they identify and make crime unprofitable through the recovery of assets (see IO.8).

199. Authorities conduct separate, parallel investigations of ML in cases where the person suspected of ML is not the same person as the one suspected of the predicate offence. This situation occurs in some professionally organised ML cases involving concealment of beneficial ownership of legal persons as illustrated in Box 3.4, even though professional money launderers are rare in Finland.

Box 3.5. Case Violet

This tax fraud case including ML was ongoing at the time of the on-site. It is the largest grey economy tax fraud case in the past ten years. The total value of the tax fraud is estimated at EUR 4. 6 million for 700 undeclared workers.

The predicate offences suspected are, among others, aggravated tax fraud, aggravated employment pension insurance premium fraud, book keeping offences, registrations offences, aggravated fraud, and aggravated ML. The ML offence suspicion is based on the fact that the suspects hid the proceeds of suspected crime by buying real estate in Turkey, following the transfer of large amounts of cash in that country.

The investigation was initiated on the basis of collaboration between NBI intelligence officers and specialist tax inspectors. The NBI also worked closely with specialised financial crime prosecutors, insurance companies, local police, real estate operators, and auditors. NBI has worked together with the Baltic States and mainly Estonia, where most of the workers came from. There is a joint investigation with Estonia, and several interrogations were held abroad through MLA.

The main suspects were arrested in November 2015 after several month of tactical surveillance and telephone tapping. The investigation was long and complex as strawmen were used, and the main suspects encrypted their communications, which made the gathering of electronic evidence difficult.

The Police (NBI) seizure decisions of EUR 4. 53 million gross resulted in seizures of approximately EUR 200 000 net.

200. Finnish investigators have appropriate skills and experience in investigating ML. There are good tools and techniques available for the investigation of ML offences. In addition and when necessary, the Police forms joint investigative teams on serious predicate offences and ML offences at the European level (see Boxes 3.4, 3.6 and 8.6 in IO.2). Finland has also demonstrated its capacity to mobilise experts from other administrations (tax inspectors for instance) in more complex ML cases (see Box 3.4).

201. LEAs have conducted a number of effective investigations on serious and complex cases with an international dimension, as illustrated in Boxes 3.4, 3.5, and 3.6). Most cases involved natural persons but cases related to legal persons and complex and organised structures were also investigated. LEAs also investigate ML based on foreign predicate offences, involving the transfer of money and subsequent retransfer, with an assumption that the money is criminal proceeds (e.g. Boxes 3.6 and 3.8). The number of criminal investigations related to ML offences (see Table 3.10) is relatively high in relation to the country's ML risk situation.

Box 3.6. Case Motorhead

There is an ongoing investigation by the NBI into several cases of aggravated fraud aggravated embezzlement, aggravated tax fraud, aggravated dishonesty by debtor, aggravated ML, aggravated accounting offence and registration offence.

The case started on the basis of international co-operation between LEAs. A foreign LEA had conducted an investigation against X and during the investigation money transfers to Finland were identified.

The companies that are the subject of the investigation are registered in Finland, Estonia, Sweden, Norway, the UK, the Netherlands and Bangladesh. The NBI has made co-operation requests in this matter to Bangladesh, Canada, the UK, Estonia, Norway, Sweden, Denmark and the Netherlands.

NBI seizure decisions of EUR 903 900 gross resulted in seizing the entire equivalent amount in net value.

Box 3.7. Case Manse

This is an ongoing and long-term ML investigation which started with an Interpol message sent by Germany to Finland, based on suspicious money transfers from Finland to Germany, and further transferred to Panama.

Crimes under investigation are aggravated embezzlement, aggravated tax fraud, aggravated accounting offence, aggravated ML, aggravated bribery in business life, and bribery in business life. The NBI worked in close collaboration with the Finnish Tax Administration, the Prosecutor's Office (Inland) Finland and the Enforcement Office (Inland) Finland.

A joint investigation team between Finland and Germany was established with the help of Eurojust at the end of 2014, and is still operating. Italy joined the joint investigation team at the end of 2016. Finland sent MLA requests to Russia and Panama.

The NBI seizure decisions of EUR 867 242 gross was based on the value of identified property. The NBI released the seizure after the decision on the tax debt was confirmed. The property which had been the subject of the seizure by the NBI was subsequently subjected to enforcement measures based on the tax debt decision.

Table 3.10. Criminal investigations related to ML offences in 2012-2017

Money Laundering Type	2012	2013	2014	2015	2016	2017	Total
ML	146	92	133	91	256	261	979
Aggravated ML	80	87	80	79	131	163	620
Attempted ML	8	6	4	4	3	4	29
ML violation	0	4	5	4	6	3	22
Negligent ML	1	3	3	4	5	7	23
Attempted aggravated ML	1	0	5	5	2	8	21
Violation of the obligation to report ML	2	1	0	0	0	0	3
Total	238	193	230	187	403	446	1 697

Source: FIU

202. Even though Finland has to a large extent an effective system to identify and investigate ML, some practices could limit the opening of criminal investigations for ML:

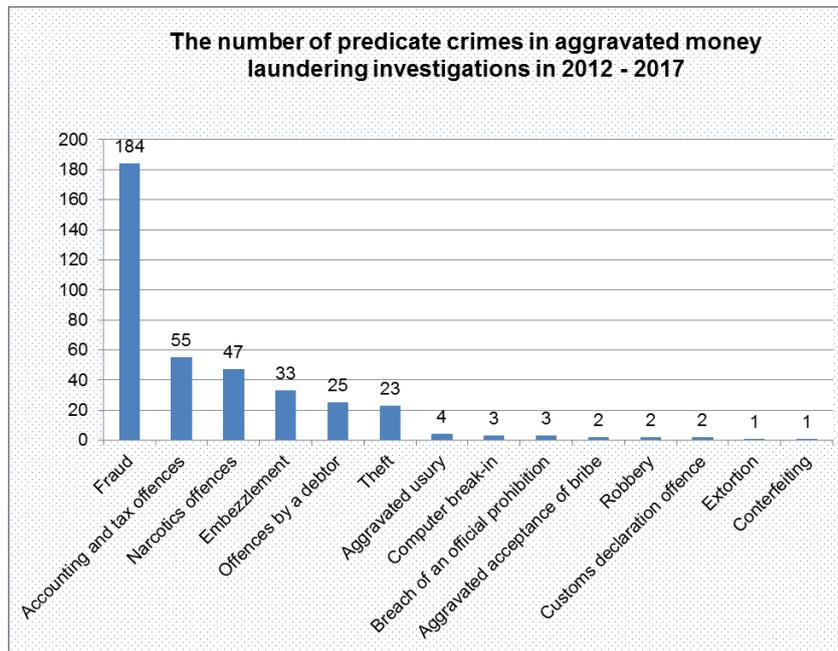
- The opening of criminal investigations does not require certainty or high probability, but just a reason to suspect that an offence has been or will be committed. LEAs therefore have very wide possibilities to investigate. When assessing this reasonable suspicion, the investigator, working in close cooperation and consultation with the prosecution services along the process, focuses on whether or not all the missing elements of the offence are likely to be resolved in the criminal investigation. This appears to be a more restrictive approach than the reason to suspect requirement, which can have an impact on the Police's decision to open a criminal investigation. The "rule of concurrent offences" (see further below) can also impact the decision to prosecute ML separately from the predicate offence, and therefore affect the opening of ML criminal investigations;
- There is limited involvement of the FIU in the dialogue between the Police and prosecutors, before the Police decides to initiate a criminal investigation. This could also affect the focus and prioritisation on ML cases.

Consistency of ML investigations and prosecutions with threats and risk profile, and national AML policies

203. The main risk of financial crime in Finland stems from the grey economy. The main ML threat in this respect is the laundering of proceeds resulting from non-payment of statutory payments and taxes, as well as tax fraud. Proceeds of drug crimes and proceeds generated from both domestic and foreign frauds are the other highest ML risks in Finland. A significant part of the proceeds generated in Finland are being moved outside of the country. Main ML methods are the use of front companies, complex corporate structures and front persons, cash couriers and wire transfers (see IO.1).

204. Finland is effectively taking a number of actions consistent with its main threats and risks in terms of number of investigations, prosecutions and convictions. Many of the more significant ML investigations (in terms of size and complexity) originate from investigations into property crimes, especially aggravated fraud and tax offences. Simpler ML cases originate from police investigations of other predicate offences, especially narcotics offences.

Figure 3.1: Predicate crimes in aggravated ML investigations in 2012-2017



Source: FIU

205. In Finland, the property crime most subject to ML is typically aggravated fraud. Other types of property crimes include embezzlement, robbery, theft, counterfeiting, usury, extortion and data protection offences. The share of property crimes as the predicate crime type in the subject period was 65% (251). The second largest crime type was financial crimes with a 22% share (85). These included accounting offences, tax fraud, customs declaration offences, dishonesty by a debtor, and breach of official prohibitions. Of the predicate crimes, only 12% (47) comprised narcotics offences. This is in line with the fact that narcotics crimes investigated are most of the time linked to individual drug dealers and are not reflected in investigations of aggravated ML. Actions towards ML offences related to drug trafficking by organised crime groups should intensify, and not only on the predicate offence.

206. As regards prosecutions and convictions, available statistics on cases of aggravated ML offences demonstrate consistency with the risk profile, as illustrated in Table 3.11. Due to the lack of relevant and comprehensive statistics, it is not possible to check if investigations, prosecutions and convictions are consistent or not with the country's risk profile, in terms of financial amounts involved.

Table 3.11. Predicate offences for indictments and convictions of aggravated ML in 2015-2016

Predicate offences for indictment	Number	%	Predicate offences for convictions	Number	%
Fraud	57	45%	Fraud	24	41%
Embezzlement	12	9%	Embezzlement	9	16%
Offences against public finances	5	4%	Offences against public finances	1	2%
Offences by a debtor	10	8%	Offences by a debtor	5	9%
Narcotics offence	13	10%	Narcotics offence	5	9%
Theft	18	14%	Theft	7	12%
Other	8	6%	Other	5	9%
Unknown	4	3%	Unknown	2	3%
TOTAL	127	100%	TOTAL	58	100%

Source: FIU

Types of ML cases pursued

207. The ML offence in Finland covers all predicate offences and meets most requirements of the Vienna and Palermo Conventions (see TC Annex, R.3). One of the main technical limitations relates to self-laundering criminalisation (see c. 3.7). However, its impact on the effectiveness of the system is limited, since self-laundering is criminalised as a separate offence in circumstances where the conduct would constitute aggravated ML, and when the blameworthiness of the ML offence prevails over the predicate offence. It should also be noted that the threshold for aggravated ML is low (EUR 13 000)⁶², which limits the negative impact of this deficiency.

208. Based on the studies conducted by Finnish authorities (see section below), there have only been a few prosecutions and no convictions of self-laundering in aggravated ML cases by the District Courts during 2015 and 2016. Those Courts issued a total of 300 judgements in which charges have been brought for any ML offence. A total of 71 judgements concerned charges for an aggravated ML offence. Out of these 71 judgements, only four with a total of six defendants concerned self-laundering. The charges for self-laundering were dismissed in all cases and it was concluded in three of those cases that the amount involved for the ML offence was the same amount as the predicate offence and therefore did not form the most essential and blameworthy part of the offence to merit a separate punishment for

⁶² EUR 13 000 has been defined as the monetary threshold for the aggravated offence in the legislative preparatory works, but this is not a legal nor strict limit as the intentional element, the complexity of the arrangements to conceal proceeds of crime also contribute to qualify an ML offence as aggravated, even when the monetary damage is less than EUR 13 000.

ML⁶³. This means that there was no conviction for self-laundering for aggravated ML during 2015 and 2016.

209. The rule of concurrent offences has a particular impact on the prosecution of self-laundering for aggravated ML cases. This rule means that where there is one criminal act by the same person that constitutes a violation of more than one criminal provision, prosecutors will prosecute the more serious crime. The authorities pointed to the possibility that the prosecutor would pursue only the self-laundering offence when he/she thought that the predicate crime would not be confirmed in court, but he/she had enough evidence to prove the criminal origin of the money handled by the defendant. This rule also has a potential impact on the decision to open ML criminal investigations (see above).

210. Finland has pursued different kinds of ML offences, despite the fact that the prosecution and sentencing system make it difficult to establish and distinguish if in a particular case the defendant has been convicted for ML.

211. Authorities do pursue ML linked to various predicate offences (tax crimes, fraud and narcotics particularly), and third-party ML. There are also a few examples of large-scale third party ML (see Boxes 3.6 and 8.4) and some standalone ML cases (see Box 3.7). The number of stand-alone cases is more restricted as most of the time there is an integrated ML investigation within the investigation of predicate offences (as opposed to parallel ML investigations, see above). Authorities also pursue foreign predicate offences (see Boxes 8.4, 3.5, 3.6, 3.7, and 3.8).

Box 3.8. Bad Apple

In 2014, the FIU received an STR as a result of which a two-year process was started. Investigations were launched into a currency transfer service provider's agent. There was reason to suspect that the agent committed aggravated ML activities. The FIU worked in close co-operation with the local police responsible for the criminal investigation.

After the criminal investigation, the case was heard at the Central Ostrobothnia District Court in June 2015. The defendant was sentenced for aggravated ML to a suspended sentence of imprisonment for one year and six months. The prosecutor appealed the District Court judgment and claimed a longer term of immediate imprisonment. The Court of Appeal of Vaasa pronounced a judgment in the case on 20 December 2016. It accepted the reasons of the District Court concerning the evaluation of the evidence, and the result of the evaluation. It sentenced the defendant to two years' imprisonment.

⁶³ In one other case, there was not enough evidence to establish the ML offence. In another case, the act was not considered ML as the property in question was not considered as proceeds of crime and the person was sentenced for the predicate offence.

Box 3.9. New Zealand

The NBI is currently conducting a preliminary investigation on a suspicion of an aggravated ML offence concerning a foreign company, allegedly a front company. The case involves significant amounts of cash transfers through cash couriers. The foreign predicate offence has not been proved yet, and the investigation is now relying on exchange of information with foreign states.

NBI seizures were EUR 3.6 million net.

212. Investigations on ML offences result in cases brought to the prosecution service based on “*probable cause*” that an ML offence was committed, and then to courts, in a majority of cases, based on elements supporting the existence of an ML offence “*beyond reasonable doubts*”. Statistics available are however limited to establish a reliable ratio of charges over investigations received by the prosecution services.⁶⁴ It appears however that investigations led to indictments to some extent, as the overall ratio of indictments in relation to the ML cases received by the Prosecutor from the Police has been estimated at around 72% from 2013 to mid-2018, according to the statistics of the Office of the Prosecutor General. During that period, prosecutors have brought to court in total 833 ML cases, of which 346 were cases of aggravated ML. Concerning cases of aggravated ML, there have been 37 decisions where charges were not brought and 13 decisions in which the investigation was restricted.

213. Cases brought to the courts by the prosecution lead to convictions in 70% of the cases, which is consistent with the average ratio of prosecutions leading to convictions in other criminal cases. In comparison the same ratio of prosecutions leading to convictions in all criminal cases has varied between 66 – 63 % in 2013 – 2018. In tax offences, the number has varied between 68 – 82 %.

214. The fact that ML offences will be co-penalised in many cases with the predicate offence may present a disincentive to prosecute ML separately. Judges’ verdicts may combine different criminal activities into one conviction. This suggests that stand-alone ML activity is considered by courts in more cases than the statistics would suggest. This sentencing practice allows for punishing the predicate and ML offence concomitantly, so it has the potential to frustrate prosecutors’ efforts in pursuing stand-alone charges of ML in non-third-party ML cases. This might have an impact in cases where the predicate offence is a crime that usually involves more complex ML schemes as investigation and prosecution could miss the ML scheme by focusing on the predicate offence. This can have an impact on the overall effectiveness of the system including when money is laundered abroad, which is most often the case in Finland’s cases.

215. The conviction statistics for ML offences do not entirely reflect the total number of ML convictions due to the rule of concurrent offence sentencing. This means that the person punished for the predicate offence is also punished for the facts that constitute ML but only the predicate offence is mentioned in the sentence (e.g. concealing the proceeds of one’s own narcotics offence is punished as part of the narcotics offences). Therefore, the number of persons sentenced for ML offences is not the only element indicating how many persons were sentenced for this

⁶⁴ It is noted that in many cases, a single prosecution or court file is based on several different investigation files.

behaviour as sentences for the predicate offences must also be taken into account. The number of prosecutions and convictions for standalone aggravated ML offences as illustrated in Table 3.11 is therefore only a proxy.

Effectiveness, proportionality and dissuasiveness of sanctions

3

216. Penalties for ML offences do not allow full sentencing proportionality as cumulative fines may be ordered only in conjunction with conditional imprisonment but not in conjunction with unconditional imprisonment (see c.3.9). The penalty scale for a basic ML offence is either a fine or a maximum of two years of imprisonment. The penalty scale for aggravated ML is at least four months and at most six years of imprisonment, and an additional ancillary fine is only possible if conditional imprisonment by itself is deemed an insufficient punishment. This limits the range of sanctions available for greater or lesser breaches, i.e. the sentencing proportionality, which is particularly relevant in the context of Finland's sentencing practices explained below. This has to be read in the specific context of Finland, where the criminal sanctions model is less coercive and the level of criminality is low (see Chapter 1).

217. A comprehensive assessment of ML sentences in Finland is hindered by joint punishments and the concurrent rule applied by courts. However, the Court of Appeal of Helsinki conducted a study in 2015 on the imposition of penalties in the context of financial offences, and in ML offences. The FIU has also conducted a study focused on charges brought for aggravated ML (standalone cases) that were tried by the District Courts in 2015 and 2016.

218. These analyses show in particular that, when the ML offence is co-penalised with the predicate offence, the extent to which this leads to an additional sanction is unclear. While the ML offence may be an aggravating factor in the sentencing, judges determine sentences based on a wide range of elements relevant to each individual case, and do not record what effect the ML activity specifically has on the final penalty.

219. Courts do not use the full range of penalties available and sentencing practice is lenient. This is particularly accurate for aggravated ML cases, in which the amount of funds laundered in the 11 cases studied by the Helsinki Court ranged from EUR 18 551 to EUR 682 775. In those cases, the sentences ranged from 5 months of conditional imprisonment to 3 years of imprisonment for the case with the highest amount. As illustrated in Table 3.12, most imprisonment sentences for aggravated ML in 2015 and 2016 were below one year of imprisonment (88%), amounting to not even one sixth of the maximum sentence.

220. Sentencing for aggravated ML in 2015 and 2016 is particularly lenient and not proportionate, including in the most complex cases, as Table 3.13 also illustrates. Imprisonment sentences were unconditional in only two cases out of 36, and in these two cases, imprisonment was replaced in practice by community service. In addition, for cases involving the highest amounts (over EUR 100 000), only one case out of five was sentenced with unconditional imprisonment (a two-year sentence). The remaining four cases were sentenced with one-year conditional imprisonment on average, with the shortest sentence being only six months (close to the minimum sentence). The proportionality of sentencing is also limited by the fact that the

Criminal Code allows for fines only as an ancillary sentence for aggravated ML and when conditional imprisonment is deemed insufficient.

Table 3.12. Length of sentences of imprisonment for aggravated ML in 2015 and 2016
(joint punishments excluded)

Sentence	2015	2016	Total
1-3 months		1	1
4-6 months		17	17
8-10 months	5	9	14
Over 1 year	1	3	4
Total	6	30	36

Source: FIU

Table 3.13. Length of sentences of imprisonment for aggravated ML in 2015 and 2016
in relation to the value of the assets laundered (joint punishments excluded)⁶⁵

Value of the assets laundered (EUR)	Conditional	Average length	Shortest sentence	Unconditional	Length
Under 13 000	1	6 months	6 months		
13 000 – 50 000	14	6 months	4 months	1	4 months
51 000 -100 000	14	8 months	4 months		
Over 100 000	4	1 year	6 months	1	2 years

Source: FIU

221. As regards basic ML offences analysed in the Helsinki Court's study, the sentences ranged from 40 day-fines to five months of imprisonment. In two cases in which the length of the sentences was five months, other offences were attributed to the offender. In cases pertaining to a ML offence alone and for which the sanction was imprisonment, the amount of funds received was about EUR 10 000 and the length of the sentence was 3 – 4 months. Sanctions were taken against a legal person in only one case in 2017 (corporate fine for aggravated ML).

222. In addition, the impossibility to order value-based confiscation for ML offences when assets laundered are untraceable reinforces the lack of dissuasiveness of the sanction regime (as described under IO.8).

Use of alternative measures

223. The concurrency rule means that where there is one criminal act by the same person that constitutes a violation of more than one criminal provision prosecutors can only prosecute the more serious crime. This means that prosecutors often indict the offender with the predicate offence before the ML offence where the former leads to a higher sanction. If during the investigation of a co-ordinated ML offence, evidence of the predicate offence is established, then prosecutors will look to charge for conspiracy on the predicate offence, which will lead to more powerful sanctions. If the predicate offence and the ML are committed by different persons or if the ML

⁶⁵ Only 35 cases (and not 36 as in Table 3.12) as one case was deemed N/A for the breakdown by amounts.

can be prosecuted as self-laundering (in accordance with Chapter 32, Section 11, para. 1 of Criminal Code, see above) both offences are prosecuted.

224. In the area of economic crime, it is common for ML activities to be prosecuted as tax offences and/or accounting offences, or as accessories to such crimes. Finland has provided many cases where authorities used alternative measures to pursue ML activities. The case provided in Box 3.9 is an illustration of tax fraud being pursued as an alternative ground for ML.

225. However, the fact that ML offences are, in many cases, investigated together with the predicate offence may also encourage investigators to focus on predicate offences considering the difficulty in reaching the level of evidence for ML offences (see above). In that context, this can be considered as having a negative impact on the importance of ML, and, to some extent, as a substitute to ML investigations and convictions.

Box 3.10. Case Lindhom

This is a VAT carousel case, in which the defendant was charged for aggravated tax frauds and aggravated bookkeeping offences. The defendant was contacted by a person in Estonia to establish a limited liability company in Finland for export and import business between Estonia and Finland, with no real operating business. The company was used in the context of a VAT carousel scheme. The defendant was condemned to imprisonment for over three years and ordered to pay compensation to tax authorities.

Overall conclusions on IO.7

226. **Finland has achieved a substantial level of effectiveness for IO.7**

Immediate Outcome 8 (Confiscation)

Confiscation of proceeds, instrumentalities and property of equivalent value as a policy objective

227. Finland pursues confiscation as a policy objective. The Finnish Criminal Investigation Act provides that in all criminal investigations, at an early stage of the process, the possibilities for the return of property obtained through the offence and for enforcement of forfeiture/seizure should be ordered as a consequence of the offence or for compensation to be paid to an injured party (Chapter 2) (see IO. 7).

228. In 2017, the freezing measures that can be ordered by the FIU to prevent the flight of assets were extended from five to 10 working days (FIU Act, Section 6). Additionally, the possibility to take freezing measures and possibly confiscate criminals' assets is part of the top criteria defined by the FIU to prioritise cases (see IO. 6).

229. Finally, under the 2016/2020 Action Plan for the Prevention of the Grey Economy and Economic Crime (see Chapter 1), finding means to improve the recovery of proceeds of crime, both in national and international contexts has also been planned. A co-operation project between relevant authorities (Enforcement,

Prosecution, Criminal Investigation and Taxation) to enhance the tracing, safeguarding and confiscation of the proceeds of crime is ongoing.

230. Despite their high-level engagement and legislative improvements, Finnish authorities do not have enough systematic data to demonstrate and assess whether the policies are actually successful in leading to decisions in courts. There are some global figures on proceeds of crime confiscated through Finnish court decisions over the last years, which support the commitment to go after criminals' money (see Table 3.14). However, there is no data available for ML/TF cases, although cases mentioned by Finnish authorities indicate that confiscations are imposed.

Table 3.14. Global confiscations ordered by court decisions, for all crimes

	2015	2016	2017
Confiscation of property n° decisions	2 523	2 271	2 056
Confiscation of funds n° decisions	1 750	1 705	1 751
Million EUR	34, 2	35,5	22,3

Source: Finnish authorities

Confiscation of proceeds from foreign and domestic predicates, and proceeds located abroad

231. Finland has developed a far-reaching system to recover assets, based on the measures and policy priorities described above. As a first step, administrative freezing orders are made by the FIU at the early stage of the investigation. Assets are systematically frozen by the FIU for 10 days to help swiftly freeze possible proceeds of crime and prevent them from being put beyond the reach of the authorities. Table 3.15 shows that the FIU orders the freezing (and seizure) of significant amounts and value.

Table 3.15. FIU orders to suspend transactions

	2015		2016		2017		Total	
	Number	Mil EUR						
Orders ("freezing")	16	1,3	42	1,7	34	2	92	5
Value of assets taken in possession by authorities under orders to refrain from conducting transactions ("Seizure") (EUR million)		0,9		1,1		0,7		2,7

Source: FIU

232. The FIU may order Customs or the Border Guard to freeze funds. In the period 2015/2017, there was one such order to the Customs, for EUR 109, 375, and no order to the Border Guards. The FIU may also make requests to its foreign counterparts to suspend a transaction. In 2014/2016, the FIU made six such requests: three to Hungary, one to Bulgaria, one to China, for a total value of more than EUR 1, 7 million. All of these requests, except one in Hungary, resulted in funds being returned to Finland. Additionally, one suspension was done in Estonia.

233. The second step possibly leading to the confiscation of funds/assets is the seizure order (assets) or interim confiscation value (value). These are done by the police during the criminal investigation if needed and as soon as possible, under the

Coercive Measures Act. Seizure decisions are under court control and are renewed on a regular basis during the investigation, based on the progress made in the case and the anticipated progress. Examples in Boxes 8.3. (Cargo case), 3.4, 3.5, 3.6, 3.8, and 3.10 (Toy Smuggler Case) illustrate that freezing measures are systematically ordered when ML investigations are opened.

234. Customs also have powers to seize funds that are suspected to be related to a criminal offence. Seizures are decided as part of the criminal investigations conducted by Customs (officer with power of arrest). The total amount of cash seizures decided between 2012 and 2017 was EUR 44 044 (six cases).

235. The Enforcement Authorities are in charge of enforcing seizures ordered by courts or by the criminal investigation authorities (Chapter 6 of the Coercive Measures Act). Enforcement officers (bailiffs) enforce the orders without delay and have direct and extensive powers to use coercive measures. The Enforcement Authorities also have access to all the necessary tax data concerning the debtor, which enable them to effectively identify, trace and seize assets. They can for example access the tax authorities' debtors database, the registered vehicles database, land and real estate property databases etc. The Special Enforcement Offices, which are the main enforcement authorities in ML/TF-related cases, enforced about 130 seizure measures in 2017 (97 in 2016; 112 in 2015 and 127 in 2014), and the estimated value of the seized property was EUR 42 million at the end of the year. The majority of these seizures were however not based on ML cases. The amount of property frozen by the Special Enforcement office based on TF cases (targeted financial sanctions, see IO.10) was around EUR 10 600 in mid-2018.

236. If part or all of the assets are located abroad, seizure is requested through mutual legal assistance (see IO.2). Finnish authorities recognise that in respect of economic crime, the increasing cross-border elements create many types of challenges.

237. As a 3rd step, and at the stage of prosecution, prosecutors have to request that the courts confiscate the assets which were seized. When the confiscation has been ordered by the courts, the execution is led by the Legal Register Centre (an independent authority under the umbrella of the Minister of Justice), including for international enforcement procedures. Finland demonstrated through some cases that the requests for confiscation are implemented as part of the criminal process.

Box 3.11. Examples of confiscation requests

Case Brytanay: Brytanay had received and transferred property acquired through offending in order to assist the offender in evading the legal consequences of the offence by concealing the illegal origin. This was done by opening bank accounts and receiving foreign payments, through fraudulent account transfers (phishing). The total value of amounts laundered was EUR 26 700. Brytanay had immediately withdrawn money from the accounts and transferred it through a money transfer provider to Ukraine, minus his commission. He was charged for aggravated ML, and his commission of 7 % was confiscated.

Case Toy Smuggler: a charity collected money from private donors mainly in Finland but also abroad. The collected funds were supposed to be given to orphan camps in Syria during the Syrian conflict. The head of the charity travelled to Syria via Southern Turkey and took the donated money in cash with him to Syria. The total amount of money donated during 2014/2016 was almost EUR 400 000. The head of the charity is suspected of having deposited tens of thousands of euros of the donated funds into his personal bank account in Turkey. FIU Finland was able to freeze over EUR 90 000 of funds in his possession. These funds were later confiscated. The case is presently in Court, for aggravated embezzlement, accounting fraud and illegal fundraising.

238. The total volume of funds forfeited to the state in ML court decisions has been quite limited compared to the estimated proceeds of crime and the funds seized (see Table 3.14). During 2017, EUR 149 175 was confiscated for ML, aggravated ML and negligent ML (see Table 3.16) and EUR 192 014 when adding up all other ML offences (see Table 3.17). Seventy-two decisions ordered confiscation of property, the value of which is not known, but this included one real estate property and smaller property items such as computers.

Table 3.16. Funds forfeited to the state in the court of first instance according to the main offence (only ML, aggravated ML and negligent ML)

Criminal offence	2011	2014	2017
Money laundering (EUR)	662	2 285	65 252
Aggravated ML (EUR)	183 100	669 495	19 300
Negligent ML (EUR)	5 545	9 500	64 623
Total	189 307	681 280	149 175

Source: Finnish Authorities

Table 3.17. National court final decisions on confiscation and freezing in 2017 concerning receiving offences and ML offences as main offences, including personal and joint liability

	Confiscation of property	Confiscation of money		Freezing	
	<i>decisions</i>	<i>decisions</i>	<i>EUR</i>	<i>decisions</i>	<i>EUR</i>
Receiving offence	37	44	34 555	3	303 090
Aggravated receiving offence	2				
Professional receiving offence	-	-	-	-	-
Negligent receiving offence	13	4	2 590		
Receiving violation	5	9	5 000		
ML	9	60	65 252		
Attempted ML	-	2	494		
Aggravated ML	2	7	19 300	1	750 000
Conspiracy for the commission of aggravated ML	-	-	-		
Negligent ML	4	11	64 623		
ML violation	-	1	200		
Total	72	138	192 014	4	1 053 090

Source: Finnish Authorities

239. These limited confiscation results have to be read in the broader Finnish context, where the seized amounts are compensated to the victims as a matter of priority over confiscation to the state. Compensation amounts are not confiscated before being handed over to the victims and therefore compensation decisions are not reflected in the confiscation statistics. Tax authorities are included in the parties which can claim for compensation, if they do not succeed in collecting tax debts. It is assumed that a substantial part of the amounts seized by Finnish authorities benefit to tax authorities, given that a substantial part of ML predicate offences are tax-related offences (see 10.7) and compensation is done on the basis of the predicate offence. Some other significant compensation cases have been mentioned, especially in fraud cases (see example in Box 3.11). The NBI succeeded in returning approximately EUR two million to victims of fraud-related schemes in 2016. In both cases, whether the final court decision is a compensation or a confiscation judgement, criminals are deprived from their assets, on a permanent basis.

Box 3.12. Example of compensation decision

C was prosecuted for aggravated ML. The predicate offense was embezzlement. In 2016, C was convicted and sentenced to unconditional imprisonment, as well as to the payment of damages to the complainants totaling EUR 662 067. 10.

240. In addition, Tax authorities confiscate substantial amounts, through court orders, when confiscation is done to secure tax debts (2015: EUR 5. 6 million; 2016: EUR 4. 9 million; 2017: EUR 1. 5). This means that these funds are out of reach for laundering or other criminal purposes.

241. Authorities do not have the ability to confiscate property of corresponding value for ML, aggravated and negligent ML (see TC Annex, R. 4). However, the value of the target of ML can be confiscated as the value of proceeds of the predicate offence without criminal conviction. This approach has been applied by courts and examples of cases were mentioned, for example a 2010 judgement of the Helsinki District Court which decided that a property worth EUR 80 000, which could not be confiscated as the target of ML due to a lack of evidence, was nonetheless confiscated as the value of proceeds of crime.

242. The extended confiscation process, introduced in the Criminal Code in 2001, is an additional tool to deprive criminals of their assets. Through this process, the offender's property can be confiscated without the necessity to establish the offence the property was derived from (see TC Annex, R. 4). A reversed burden of proof applies, i.e. the offender has to prove the licit origin of the assets in order to avoid confiscation. This process tends to facilitate the assets recovery process as it requires less evidence for the offence than "regular" confiscation. However, Finland did not demonstrate through cases how this process was used in ML-related cases. In addition, there is a condition that the property is clearly derived from criminal activity that is not considered insignificant (see TC Annex, R. 4).

243. Mechanisms are in place in Finland to help authorities and courts deprive criminals of their assets. However, the technical limitations identified in these processes and the lack of evidence or illustration on how this is regularly, consistently and successfully applied in practice impact the assessment of the effectiveness of the system. This is especially so in the specific context of Finland, where a significant part of proceeds of crime generated domestically are moved outside of the country (see IO.1) and therefore may not be easy to recover. In cases where ML proceeds have not been seized or frozen at the criminal investigation stage because they were already sent abroad, implementation of court decisions to confiscate will be hindered and rely heavily on international co-operation. The limited number of prosecutions, both in ML and TF cases (see IO.7 and 9), also has a direct impact on the confiscation levels.

244. Confiscations in cross-border ML cases and repatriation of assets to Finland are insignificant. A substantial part of the proceeds of crime in Finland is moved out of the country (see IO.1). Finland does not have comprehensive statistical data regarding the confiscation decisions made in cross-border ML cases. The Legal Register Centre provided a representative set of requests it sent to other EU Member States with which criminal flows are the most significant (i.e. Estonia, France, Spain, Netherlands) in 2015, 2016 and 2017 following confiscations decisions made by Finnish Courts. Most of these conviction and confiscation decisions were made on predicate offences (narcotics offences and fraud mainly). Only a limited number of cross-border confiscation decisions were made in ML cases, with low amounts repatriated to Finland. Significant orders were refused as the execution was barred by the statutory time limitations.

Table 3.18. Sample of decisions on requests for repatriation in Finland of confiscated funds

EU Member State	Offence	Requested amount (EUR)	Present status	Repatriated to Finland (EUR)
Spain (Request sent in 2012), see Box 3.12 for more details	Aggravated ML (predicate offence: fraud)	23 269	Enforcement completed	23 263, 23
Estonia	Aggravated ML (predicate offence: aggravated theft)	55 000	No response from Estonia so far	
France	Attempted ML (predicate offence: unknown)	246 000	Decision on the enforcement expected in fall 2018	

Source: Legal Register Centre

Box 3.13. Example of confiscation order implemented by Finland in accordance with the EU Confiscation Framework Decision

A was prosecuted for aggravated ML. A was targeted for a house search in 2007 in Spain. A total of EUR 23 269 was seized in connection with the search. In 2009, the District Court of Helsinki ordered the freezing (“*seizure for security*”) of A’s property corresponding to the total amount of EUR 598 129,13. The decision had been transmitted to Spain, where, by decision of the Fuenlabrada court in Madrid, A’s funds were seized for the amount of EUR 23 269.

In 2011, the District Court of Helsinki convicted A for aggravated ML, in accordance with the prosecutor’s charge, and sentenced to unconditional imprisonment. A was also sentenced to lose the economic benefit of the crime (confiscation) totalling EUR 70 953,50 to the Finnish state. A was also sentenced to lose the seized sum of EUR 23 269 to the Finnish state. In 2012, the Legal Register Centre issued a request for enforcement of the confiscation order to the Spanish competent authority in accordance with the EU Confiscation Framework Decision. In 2015, the Legal Register Centre received funds frozen from Spain totalling EUR 23 263. 23.

Confiscation of falsely or undeclared cross-border transaction of currency/BNI

245. Confiscation in cross-border cash-transportation cases is not applied to a satisfactory extent. Customs and the Border Guard temporarily freeze the amount of money transported following a FIU order (see above) or whenever a prior cash declaration is absent or false. However, if this amount is not directly connected or cannot be linked with another predicate offence enabling the authorities to open a broader criminal investigation, it will be released to the owner after the payment of a fine (see TC Annex, R. 32). Based on the examples provided by Finland, the fines applied (see Box 3.13), based on the day fine approach (see TC Annex, c. 32.5), do not lead to effective, proportionate and dissuasive sanctions, especially with regard to the amounts of undeclared cash detected.

Box 3.14. Examples of fines applied for undeclared cross-border transaction of currency

A targeted customs control was performed in March 2018. A total amount of EUR 75 458, 82 undeclared cash was found. Twelve day fines were imposed (the amount of a single day-fine was EUR 21) and the total amount of fines was EUR 252.

The targeted customs control of a flight from Istanbul was organised in February 2018. One of the passengers was marked by a sniff dog, interviewed and frisked. EUR 20 000 undeclared cash was found in the passenger's pockets. Ten day fines were imposed (the amount of a single day-fine was EUR 35) and the total amount of the fine was EUR 350.

Consistency of confiscation results with ML/TF risks and national AML/CFT policies and priorities

246. There are some indicators that measures taken to deprive criminals of their assets are aligned with Finland's major ML/TF risks. A comprehensive review of Finnish court decisions in which confiscation measures were imposed cannot be conducted due to the lack of data available. Therefore, conclusions cannot be made on the consistency of confiscation measures with the ML/TF risks of Finland. As regards deprivation of assets related to TF, it is not fully in line with the country's risk profile as no effective steps have been taken to freeze assets of FTFs.

247. However, information on the cases in which the FIU has ordered suspension of transactions, and consequently (temporarily) froze funds, shows that substantial amounts relate to ML cases related to different types of frauds and a number of economic crimes (dishonesty by a debtor, registration offence accounting offence).

248. Furthermore, a sample of 2015/2017 cases with cross-border elements, where Finland made requests to other EU Member States to repatriate confiscated assets, showed that the list of countries to which most of the requests were made was in line with Finland's geographic ML risk profile (Estonia, the Netherlands, Spain, France, Germany, UK and Lithuania), see Table 3.18. However, no information was available for cases involving non-EU countries.

Overall conclusion on IO.8

249. **Finland has achieved a moderate level of effectiveness for IO.8.**

CHAPTER 4. TERRORIST FINANCING AND FINANCING OF PROLIFERATION

Key Findings and Recommended Actions

Key Findings

TF Investigation and Prosecution (Immediate outcome 9)

- a) TF cases are well identified, usually based on information from the FIU and Finnish Security Intelligence Service (SUPO).
- b) The quality of investigations is generally high and based on a collaborative approach between relevant authorities. Law Enforcement Authorities (LEAs), with SUPO's input, are able to mobilise joint investigative teams with international counterparts and use advanced investigative tools.
- c) TF investigations are in principle part of every terrorism-related investigation, but TF is not usually pursued as a distinct criminal activity. Human resources dedicated to and specialised in terrorism and TF that are available to the National Bureau of Investigation (NBI) –and in particular to the FIU – might become insufficient considering the increasing mobilisation on TF risk.
- d) TF prosecutions have been initiated, but there have been no convictions to date. This is broadly in line with the overall TF risk in Finland. However, the recent changes in the TF environment – with a strongest focus on ISIL FTFs and returnees – are not yet reflected in TF cases.
- e) The TF offence legal framework does not criminalise the financing of an individual terrorist without a link to the use of funds to finance a specific offence. This, combined with a restrictive approach to start TF criminal investigations, and limited resources available to gather evidence, limits investigations and prosecutions of TF.
- f) Prosecutions for related or other offences (e.g. VAT fraud) have been successfully undertaken as disruption tactics to address TF-related activities.

TF preventive measures and financial sanctions (Immediate outcome 10)

- a) Finland has measures in place to implement Targeted Financial Sanctions (TFS) for TF. However, implementation is not without delay nor fully effective, mainly because of technical deficiencies inherent to applicable EU regulations. Domestic provisions available to Finnish authorities to implement UNSCRs are not used as authorities assume this would not reduce, in a majority of cases, the implementation time.
- b) Finland has adopted domestic measures to implement UNSCR 1373 which enable the listing of EU internals.
- c) TFS are used only to some extent as mitigation measures, in particular with regard to FTFs.
- d) Finland has successfully frozen terrorist related assets but to a very limited extent. It has not requested other countries to take freezing actions against designated persons.

- e) Finland has identified Non-Profit Organisations (NPOs) receiving state subsidies, NPOs active in conflict zones and immigrant based NPOs as the subset of NPOs at risk of TF abuse. However, its analysis is not up-to-date.
- f) The level of awareness of these TF risks is uneven in the country. It is very good among LEAs, the FIU and SUPO, but remains insufficient for NPOs themselves and public authorities in charge of their monitoring.
- g) Finland has not provided guidance, conducted outreach activity or developed focused actions vis-à-vis potentially vulnerable NPOs and prevent their possible misuse for TF purposes.
- h) The general registration, accounting and auditing requirements applicable to all NPOs, as well as the special money collection permit, and the associated reporting obligations, are effective transparency measures to reduce the vulnerability of NPOs at TF risk. There is a good public awareness of these obligations that helps reducing the risks.
- i) Finland does not demonstrate how TF risk is taken into account in the monitoring of relevant NPOs.

Proliferation financing (Immediate outcome 11)

- a) Information sharing and co-operation between relevant authorities at the domestic level, and with international partners when necessary, is effective for the implementation and enforcement of TFS for PF.
- b) The export control authorities (Ministry of Foreign Affairs (MFA), SUPO and Customs) have a good understanding of CPF obligations, and communicate and co-operate regularly with LEAs to detect PF-related cases and start investigations, both at domestic and international level. Although a few investigations have been launched, no court proceedings have been started as the cases investigated did not involve PF breaches eventually.
- c) Finland implements TFS regarding PF through EU measures, with minor delays in the transposition of UN designations. However, in the case of Iran, the practical effect of these delays has been successfully mitigated by prior designations by the EU. In the case of DPRK, delays still exist.
- d) Financial institutions and Designated Non-Financial Businesses and Professions have a good understanding of their TFS for PF obligations and good advice and guidance is provided by authorities, particularly by the MFA. As for TFS on TF (see IO. 3 and 4), supervisors do not have legal powers to supervise or sanction for the implementation of these obligations (although this is done in practice to some extent as supervisors do check that the necessary processes are in place when conducting the licence granting process). Therefore, there is uncertainty regarding the level of compliance by obliged entities.

*Recommended Actions**Immediate outcome 9*

Finland should:

- a) Clarify the Criminal Code provisions so that the TF offence does not require a link to a specific terrorist offence when funding an individual terrorist.
- b) Increase relevant authorities' focus on ISIL FTFs and returnees in line with the identified TF risks in the country.
- c) Include more detailed actions on Counter Terrorist Financing in the updated national strategy on Counter Terrorism, in order to encourage further convergent efforts of all relevant authorities to combat TF.
- d) Increase LEAs' focus on TF investigations and prosecution, in particular through the promotion of a more proactive approach to opening TF cases.
- e) Increase professionally skilled resources dedicated to investigations of terrorism/TF offences, in the FIU, NBI and the prosecution to facilitate a more proactive approach to criminal investigations, including through training and recruiting terrorism/TF experts.

Immediate outcome 10

Finland should:

- a) Adopt a clear legal basis to ensure implementation of the UNSCR 1267 mechanism, as the scope of the Freezing Act is currently limited to UNSCR 1373.
- b) Take actions to implement TFS without delay, whether at the EU level or by using/adopting domestic provisions for direct implementation.
- c) Use TFS on a more frequent basis as a preventive or disruptive tool to mitigate the risks (especially those related to ISIL FTFs and returnees) including when criminal proceedings are either not possible or not practical.
- d) Make greater use of proposals for designation at the international level, as well as requests for freezing by other countries.
- e) Update the research on NPOs at specific risk of TF abuse and use the results to conduct training and targeted outreach. Increase dissemination to NPOs of information available about TF risks, and on methods used by terrorist financiers. Keep information level among different authorities and where needed enhance it, including the local police and the NPO sector by providing TF-risk focused trainings.
- f) Develop targeted monitoring/oversight of NPOs at TF risk.

Immediate outcome 11

Finland should:

- a) Enable TFS related to PF for DPRK to be implemented without delay in cases where the entity has not previously been listed by the EU, whether at the EU level or by using/adopting domestic provisions for direct implementation.

- b) Grant supervisory powers to all AML/CFT supervisors and Self-Regulatory Bodies of obliged entities for the supervision of the implementation of TFS for PF.
- c) Pursue training and outreach to private sector entities, with an emphasis on sanctions evasion.

4

250. The relevant Immediate Outcomes considered and assessed in this chapter are IO.9-11. The Recommendations relevant for the assessment of effectiveness under this section are R. 1, 4, 5–8, 30, 31 and 39.

Immediate Outcome 9 (TF investigation and prosecution)

Prosecution/conviction of types of TF activity consistent with the country's risk-profile

251. Finland has conducted some criminal investigations and cases involving FTFs, and money collection through NPOs, the nature of which is in line with the TF risk in the country. There were only two criminal investigations focused on TF, one in 2011 (see Box 4.2 and 4.5) and one in 2016 (see Box 4.6). No criminal investigation on financing a terrorist group has been initiated since the introduction of the offence in the Criminal Code in 2014.

252. The number of prosecutions of TF activity in Finland is low. Finland has only prosecuted one TF case, but no conviction was obtained as the Court of Appeal dismissed the verdict of the District Court of Helsinki in that case (see Box 4.1). Even if the number of convictions is lower than in several of its neighbour countries which present similar TF threat environments such as Sweden and Denmark, it remains broadly in line with Finland's TF risks.

Box 4.15. Case R 15/526 – Helsinki Court of Appeal

In March 2016, the Helsinki Court of Appeal passed a judgment to dismiss four defendants that were charged of TF and other terrorist offences. In addition, one of the defendants was charged with recruitment for the commission of a terrorist offence and with preparation of an offence committed with terrorist intent.

The defendants were accused of having remitted their own funds or funds collected for this purpose to Somalia and Kenya to be used for terrorist activities by Harakat al-Shabaab al-Mujahideen (al-Shabaab) between 2008 and 2010. According to the charge, the accused had collected small sums of money from many different people and remitted them to persons who were either involved in the activities of al-Shabaab or had some other close connection to the organisation. The amount of money collected and remitted at a time varied between USD 35 and 360. One of the defendants had sent a higher sum of money, a total of USD 2 500 in five instalments.

The District Court considered it established that al-Shabaab had committed terrorist offences specified in the Criminal Code of Finland at the time of commission. It also stated that terrorist activities and their expenses had such a significant role in al-Shabaab's activities as a whole that it had to be considered that the funds remitted to the organisation had been used for financing terrorist activities. The District Court considered that the defendants had been aware that the funds would be used for financing Al-Shabaab's terrorist activities when they collected or remitted them. Furthermore, the District Court considered that all defendants knew, in January 2009 at the latest, that al-Shabaab's activities had a terrorist intent. The defendants were initially sentenced for TF by the District Court with conditional imprisonment.

The defendants appealed against the District Court judgment on the ground that the funds were intended for poor people as alms or other forms of charity or assistance. The Court of Appeal considered that the applicable legislation in force at the time of commission required that the defendants would have had to be sure or completely clear, that the funds they collected or remitted would be used for committing specific terrorist offences, even if such offences were not in reality committed.

It was an established fact that there was a civil war going on in Somalia at the time in question and that al-Shabaab was one of the war parties. The Court of Appeal considered that one of the defendants had been aware of the fact that the funds he remitted would be used to support al-Shabaab's combat actions. Supporting al-Shabaab's combat actions economically could not, however, be considered a proof of the defendant's intention to finance any of the terrorist offences explicitly specified in the legislation. The defendant's procedure did not fulfil the essential elements of the offence as defined in the legislation in force at the time of commission, which led to the charge being dismissed.

253. The TF-related investigations and prosecutions do not reflect the changes that affected the TF environment over the past years, which now focuses on risks related to ISIL and FTFs (see IO.1 and Box 4.2). Finland still considers these risks to be too recent in nature to lead to concrete TF cases. The Turku attack in August 2017 by an ISIL fighter has contributed to the change of the authorities' appreciation of terrorism and TF risk in Finland, both in terms of nature and level. However, case examples presented during the on-site visit showed that the TF risks related to conflict areas appeared before 2014, also in Finland.

Box 4.16. Foreign Terrorist Fighters (FTFs), as one of the main TF risks in Finland

Since 2012-14, Finnish authorities have noted that the terrorist threat no longer focuses exclusively on support to participation in overseas terrorist groups. The authorities estimated that around 80 FTFs have left Finland for Syria, and about 30 have since returned to Finland or other European countries. FTFs and particularly returned FTFs make up the most significant terrorist threat and TF threat in Finland - both individually because they are radicalised and have received paramilitary training, and socially since they return with credibility and contacts, and can inspire or recruit others (SUPO – threat assessment 2017⁶⁶). Fundraising for FTFs is based on social networks of family and friends, as well as on petty crime, but is not large scale or organised.

254. In that context, investigations and prosecutions on TF should also have evolved to reflect this changing trend. At the time of the on-site visit, there was no ongoing TF investigation involving ISIL and FTFs that had reached the level of evidence to press charges and be presented to a judge in court.

255. As regards ISIL FTF returnees, authorities implement a case-by-case approach but no investigation has been opened yet, which is not in line with the related TF risk. Since 2014, travel for terrorist purposes, and the financing or encouragement of this act, is criminalised in Finland (see TC Annex, R. 5.2 bis). This should enable the prosecution of some FTFs and their facilitators, but no cases have yet reached this stage.

Box 4.17. Case of Foreign Terrorist Fighters (SUNNY TRAVEL, 2013 - 2016)

In 2013, Finnish citizens (G, M, K, U, and P) converted to Islam, four of them in the same mosque. None had significant criminal backgrounds. The group made a joint decision to travel to Syria for Jihad, armed struggle and martyrdom.

In 2012, G and M had already travelled to Georgia to a training camp run by Arabic speaking Chechens. From Georgia, G and M travelled to Syria where they met their Finnish friend S who was a member of Kataib al-Muhajirin/ISIL. S became the contact person for the group.

During the spring of 2013, the group collected over EUR 100 000 through fast loans, mail frauds and VAT-fraud. The money was used to buy cars and equipment for the trip. Members of the group also established a relief organization to hide the purpose of the trip and for fund raising.

The group travelled in two cars to Turkey. During the trip, they were informed that S was killed in battle. K flew back from Turkey and never went to Syria. G, M and P joined Kataib al-Muhajirin/ISIL. U joined another armed group in Syria.

U and G returned to Finland in 2013, P was killed in battle in January 2014 and M is still in Syria.

In 2016, the District Court found G, K and U not guilty of terrorist offences, as there was not enough evidence of terrorist intent.

256. The difficulty of successfully conducting prosecutions under the limited TF offence explains the limited number of prosecutions. Even though the TF offence was amended in 2014 to include financing of a terrorist group and travelling for the commission of a terrorist offence, it stills requires - for the financing of an individual terrorist - a link to be made with the financing of these specific offences (see TC Annex, R. 5).

257. To prosecute for the financing of an individual terrorist, the prosecutor is required to establish a link with the financing of a specific terrorist offence that has been or was intended to be financed with the funds. Finnish authorities have a restrictive approach of “the use of funds” to decide to open a criminal investigation. They would only look for the existence of suspicions that funds were used in relation with or for support to terrorist activities, and would not consider funds used for any purposes (see TC Annex, c. 5.2). Considering the role of the prosecution in the opening of criminal investigations for terrorist offences, this also explains the limited number of criminal investigations as the NBI would rarely open a criminal investigation if the Prosecutor General indicates in advance that the conditions required to prosecute are not met (see Box 4.4).

Box 4.18. Opening of a Criminal Investigation and Prosecuting Terrorist Offences, including TF offences

Who makes the decision to open a criminal investigation?

- If the suspected terrorist offence has been committed **outside Finland**, the Prosecutor General decides on the initiation of the criminal investigation (Section 8, subsection 1 in Chapter 3 of the Criminal Investigation Act; Section 12, Chapter 1 and Section 7, Chapter 34a of the Criminal Code).

- If the suspected terrorist offence has been committed **in Finland**, the National Bureau of Investigation (NBI) decides on the initiation of the criminal investigation (Section 3, Subsection 1, Chapter 3 of the Criminal Investigation Act).

However, the Prosecutor General decides on the bringing of charges for terrorist related offences (Section 7, Chapter 34(a), Criminal Code). Based on the preparatory work of the Criminal Code and Criminal

Investigation Act, and as confirmed by the services of the Prosecutor General during the on-site visit, criminal investigations on suspected terrorist offences committed in Finland are therefore usually not initiated when the prosecution order will eventually not be rendered. In practice, that means that when the Prosecutor General indicates, before the criminal investigation is initiated, that she or he is unlikely to prosecute the case based on the facts and leads available for the investigation, the NBI - even if it could regardless of the opinion of the Prosecutor General - will not initiate a criminal investigation into a terrorist offence committed in Finland.

What is required to decide to initiate a criminal investigation?

- A criminal investigation is initiated when there is a reason to suspect that an offence has been committed (Section 3, Subsection 1, Chapter 3 of the Criminal Investigation Act). There is no need for certainty or high probability. The criminal investigation authority shall if necessary clarify the circumstances connected with the suspected offence in particular so that “no one is unjustifiably deemed a suspect in the offence” (Subsection 2).

- According to the Prosecutor General, when assessing this reasonable suspicion, both the law and the facts have to be considered. Regarding the law, the focus is on whether there is such a penal provision which can be applied to the assessment of the act provided that all the missing essential elements of that provision can be resolved in the criminal investigation.

258. A restrictive approach is adopted with regard to the opening of criminal investigations of TF. As is the case with ML investigations (see IO.7), the opening of criminal investigations does not require certainty or high probability, but only a reason to suspect that an offence has been or will be committed. Prosecutors, the NBI and the FIU described several situations in which TF investigations were not opened because investigators, working in close co-operation with the prosecutor, considered that they would not be able to prove the required intent with available resources to gather evidence, nor trace the final recipient of funds. Therefore, they decided not to open a TF investigation, as the case did not reach the level of practicality required by law.

259. Both the NBI and the prosecution also considers that it is seldom practical to initiate a criminal investigation when the case involves legal co-operation with a jurisdiction that is knowingly unwilling to cooperate, or when the suspect is not in Finland and it is unlikely that he/she will ever come or return to Finland. These circumstances are of particular relevance in TF cases, especially regarding FTFs.

260. In addition, limited police human resources to gather evidence seems to constrain the capacity to initiate new criminal investigations. Terrorism cases are investigated by the three NBI investigation departments (Homicide and Violent Crimes, Organised Crimes and Financial Crimes). These three units all consist of skilled and experienced investigators, but only a few of them with experience in TF and/or terrorism investigations. NBI has its own unit working on financial

intelligence. The financial investigations benefits from co-operation with other agencies including the FIU, local police, the Tax Authorities, Customs and prosecutors. The service of the Prosecutor General has one prosecutor dedicated – among other issues – to TF activities. The FIU has only one part time (50%) analyst specialised on TF that does not seem to be consistent with the increased level of risks, nor with its change in nature.

TF identification and investigation

261. The FIU is playing an effective and central role in the early identification of TF intelligence cases, and actively disseminates useful financial information to SUPO and NBI to initiate and support criminal investigations. This is based on financial intelligence identified and disseminated by the FIU as TF-related STRs. Although still limited in number, TF-related STRs are a useful source to identify potential TF cases (see IO.6). Cases opened by the FIU's power to launch an analysis case are often based on intelligence and information from SUPO. The FIU has opened a total of 157 TF cases since 2015, and two STRs have led to identifying persons not yet known by SUPO. Seven cases were also based on requests to/from foreign countries. No TF cases were initiated on the basis of information (e.g. cash controls, cross-border cash transport declarations) provided by Customs. The reason why these 157 cases did not lead to criminal investigations is a mix of the limitations of the TF-offence, investigative challenges and available information.

262. The NBI, which is the responsible authority for investigating both terrorism and TF offences, routinely includes financial information in its investigations. The FIU's analysis of STRs and other financial intelligence it collects is used by the NBI for its investigations. As is the case for ML, in TF cases, the authorities prioritise resources to "follow the money". The Prosecutors and police confirmed that the financial dimension is always part of the scope of the investigation.

263. Another source of TF investigations are the suspicions reported directly to the Police (but not to the FIU) by other authorities (namely Customs and the Tax Authorities).

Table 4.19. Suspicions of terrorist offences reported to the Police 2014 -2017

2014	2015	2016	2017	Total
7	20	6	23	56

Source: NBI

264. There is a good level of co-operation between the NBI and the prosecution during the criminal investigation phase. The prosecutor in charge of TF cases at the General Prosecutor's Office is involved at an early stage, and has regular contact with the NBI. This interaction is explained by the fact that the role of the prosecution is predominant in the NBI's decision to open a criminal investigation (see above). When opening an investigation on terrorism or TF, the prosecutor and the police/NBI establish a team and prepare a plan for the investigation.

Box 4.19. Investigation part of the Case R 15/526 (cf. Box 4.1)

The investigation was originally initiated by information received in 2009 from a foreign intelligence service. SUPO conducted a surveillance operation on multiple individuals residing in Finland and abroad. The findings, indicating a cell supporting terrorist group Al-Shabaab had been established in Finland, were presented to the National Bureau of Investigation and State Prosecutor in January 2011. The stakeholders concluded there was sufficient evidence on money transfers made with a terrorist intent and other terrorist offences to launch a pre-trial investigation in Finland. A criminal case was filed in February 2011.

A joint investigation team between NBI and SUPO was set-up in March 2011, and a state prosecutor was included in the team from the start. The investigation was led by NBI, and while investigators gathered more evidence via COMINT, OSINT, FININT and HUMINT, the detectives from SUPO focused on transforming the gathered intelligence into evidence. Several foreign authorities were included in the investigation and Requests of Mutual Legal Assistance were sent to AMISOM, Ethiopia, Kenya, Romania, United Kingdom and USA. During the investigation, the authorities received excellent co-operation from money transfer service providers in Finland and abroad.

Several individuals were arrested at the end of 2011. The case file was transferred to the State Prosecutor in January 2014, who transferred it to the Helsinki District Court in September 2014. Several individuals were convicted for financing of Al-Shabaab. The sentences were appealed to the Court of Appeal which decided, that while it was apparent that money had been sent to East Africa to support Al-Shabaab, the connection between the money transfers and specific terrorist attacks had not been established. All the defendants were found not guilty (see Box 4.1).

One of the suspects of the investigation remains on the national list of designated persons. The Finnish Penal Code was amended in December 2014 in order to criminalize providing financial assistance to a terrorist group.

265. When the NBI decides to open an investigation on terrorism and TF, it is a priority case, which benefits from the resources and technical means needed. Investigators use techniques including secret communication, surveillance, communications control, and electronic seizures - in particular of data traffic with social media- used to link the individuals to the social media account.

TF investigation integrated with – and supportive of- national strategies

266. Finland's National Counter-Terrorism (CT) Strategy includes TF aspects (see IO. 1). Finland has not developed a specific TF strategy, which is consistent with the country's overall TF risk profile. The main pillars of the 2014/17 National CT Strategy, updated in June 2016, are prevent, pursue, tackle and respond to the

terrorist threat. The pillars are reflected in the Action Plan, which focuses on prevention, including measures to counteract radicalisation and recruitment by extremist and terrorist groups. The focus is also on information-sharing, and on the development of authorities' CT understanding and knowledge. The draft government decision on the national CT Strategy 2018-2021 is under consideration and expected to be adopted during the autumn of 2018.

267. The TF pillar of the current CT Strategy is very limited and focuses only on very high-level objectives. An Action Plan to guide authorities in their investigations and prosecution of TF is also lacking. As a result, the way authorities integrate their actions to support the National Strategy is very uneven.

268. Nevertheless, TF is considered as a priority for the FIU and SUPO whose priorities include preventing terrorist attacks in Finland and the facilitation of terrorist activities elsewhere. The 2014/7 National CT Strategy is the basis for specific goals for SUPO and the NBI, set through an annual planning process.

269. The NBI develops a case-by-case approach to TF investigations but does not develop actions in the context of a broader TF internal strategy. Nevertheless, the criminal investigative work seems to be conducted based on available evidence at a very early stage. Investigations on terrorism and terrorism related offences are given high priority when the conditions to open a criminal investigation are met.

Effectiveness, proportionality and dissuasiveness of sanctions

270. As there was no conviction for TF at the end of the on-site⁶⁷, it was not possible to assess the effectiveness nor the dissuasiveness of sanctions applied by courts. However, judges met during the on-site visit indicated that sentencing practice generally remains lenient in Finland, as courts usually do not use the full range of sanctions provided by law. Most of sentences do not go beyond the first third of the possible maximum sanction. Concerns expressed in IO.7 also apply for TF offences.

271. The applicable sanctions are consistent with the sanctions applied for other comparable crimes in Finland. As noted in the analysis of technical compliance (R. 5), natural persons convicted of TF are punishable with imprisonment for at least four months and at most eight years. The same range of sanctions applies for ML or for public provocation, recruitment, or training for terrorism. The sentences for terrorist offences vary depending on the seriousness of the offence, from a maximum of 3 years for the least serious terrorist offence to life imprisonment for the most serious offence (homicide).

272. The maximum sanction for financing a terrorist group (3 years) is neither proportionate nor dissuasive, when compared with the maximum sanction for TF (at most 8 years). Finnish authorities explained that the seriousness of the financing of a terrorist group offence is not at the same level as the financing of terrorism, since the financing of terrorism more directly targets the foreseeable criminal activity, as

⁶⁷ After the on-site, on 15 June 2018, the District Court of South-West Finland sentenced a failed Moroccan asylum seeker to life in prison for murder and attempted murder with terrorist intent for the attack that took place on 18 August 2017 in Turku and killed 2 persons and severely injured 8 others. This was the first court sentence in Finland for a terrorist offence.

compared to the financing of a terrorist group. However, there should be no such difference between the financing of terrorism (by an individual terrorist) and of a terrorist group and the TF offence for an individual terrorist should not require a link to a specific offence.

Alternative measures used where TF conviction is not possible (e.g. disruption)

4

273. Finnish authorities seek opportunities to disrupt terrorist financing activity when it is impossible to obtain a conviction for the offence of terrorist financing. This is done principally through investigation and prosecution for alternative criminal offences. This is particularly relevant given the difficulty of obtaining a conviction for terrorist financing under the current legal framework (see above).

Box 4.20. Aurinkomatkat

The District Court of Helsinki convicted three persons of economic crimes (tax frauds etc.), and dismissed all charges for terrorist crimes. It found that the defendants had given false information to the tax authorities. As a result, the companies in which the suspects had operated had avoided value added tax and pension insurance payments.

The prosecutor claimed that the suspects had used the profits of their economic crimes to buy equipment and finance their travels to Syria to commit terrorist crimes there. The Court did not find evidence to support the claim of the prosecutor.

274. Disruptive cases can arise where an investigation identifies TF activity, but there is not sufficient evidence to successfully prosecute for a TF offence, or where there is an urgent need to disrupt the activity, even though evidence gathering is incomplete. In such cases, Finnish authorities explore whether it is possible to prosecute for other offences. This may involve prosecution for an alternate offence based on evidence already obtained through the investigation of the TF offence, or further investigation by another authority (with financial investigation support provided by the FIU to the relevant authority) prior to prosecution. The prosecutor from the General Prosecutor's Office decides whether the evidence collected is enough to bring charges on TF (see above). If not, the prosecutor advises whether to continue TF investigations or to pursue alternative criminal charges as a means to disrupt TF activity.

275. There have been some cases in 2015-18 where other offences have been successfully used to disrupt TF activities, e.g. for money collection offence (see IO.10), or aggravated accounting and tax crimes (See Box 4.6). The NBI liaises with other investigative bodies able to develop relevant investigations and seek convictions, including tax authorities, Customs, local police and international CT networks.

Overall conclusion on IO.9

276. **Finland has achieved a moderate level of effectiveness for IO.9.**

Immediate Outcome 10 (TF preventive measures and financial sanctions)

Implementation of targeted financial sanctions for TF without delay

277. Finland's implementation of targeted financial sanctions (TFS) against TF is not fully effective, mainly because of technical deficiencies that are inherent to the applicable framework. The Finnish framework is based on EU regulations, and national measures for designation and freezing under UNSCR 1267/1988 and 1989 and UNSCR 1373 (see TC Annex, R.6). This affects the effectiveness of the designation system in Finland.

278. TFS under UNSCRs 1267/1988 and 1989 and subsequent resolutions are not implemented without delay. This is due to the time taken at EU level to transpose new UN designations into the relevant EU legal instruments. These delays have reduced in recent years: in 2017, transposition of designations under UNSCR 1989 took 1-7 days. Since 2015, an expedited procedure has been adopted by the European Commission for implementation of new listings, which has reduced the delay to approximately 4-11 working days of the UN decision. Nevertheless, even the shortest possible time for transposition into EU law is not consistent with the requirement to implement sanctions without delay.

279. Even though Finland has legal provisions that would enable it to implement UNSCR obligations directly by decree without relying on the EU implementation process, authorities do not use them in practice. Authorities do not use the provisions of the Act on the fulfilment of certain obligations of Finland as a Member of the United Nations and of the European Union ("Sanctions Act"), and wait until the EU process is completed. Authorities claim that, in a majority of cases, the government decree making process would not shorten the EU delay of implementation. However, this has not been demonstrated in practice. Implementation without delay therefore remains an impediment to Finland's effectiveness.

280. The legal mechanism to identify targets that fall under the UNSCRs 1267/1988 and 1989 regimes and to make proposals for designation is not clear in Finland. As detailed in the analysis of R.6, the Freezing Act is not directly related to the implementation of UNSCR 1267/1988 and 1989 as it lays down provisions on the freezing of funds only for the purpose of implementing UNSCR 1373 obligations (Freezing Act, Section 1).

281. However, in practice persons and entities designated under UNSCR 1267/1989 would - in almost all cases - also meet the criteria under the Freezing Act which refers to terrorist offences. In these cases where the person or entity suspected of, charged with or convicted of such a crime is linked to ISIL or al-Qaeda, the listing criteria of 1267 sanctions regime can be met and the mechanism for designation for UNSCR 1373 would apply. In other - more seldom - cases, it is however not clear which legal basis would apply even though it is noted that the MFA is the authority in charge of the duties imposed by the EU and UN (see TC Annex, R. 6).

282. Finland has never designated any person under UNSCR 1267/1988 and 1989. It is therefore uncertain whether this mechanism could apply and be used.

283. At the national level, Finland has a legal framework to freeze the funds/assets of individuals or entities under UNSCR 1373 which targets EU internals. EU internals are covered by the Freezing Act which provides that the funds/assets of a natural or legal person listed under the EU Council Common Position (CP 931/2001/CFSP) and not covered by the EC Regulation (2580/2001) are subject to freezing. Requests from third countries would be considered under EU mechanisms, as well as by the Freezing Act. Finland has never received a freezing request from another country.

284. Finland is using TFS as a tool for managing TF risks to a limited extent. Finland has made use of TFS, on the basis of the Freezing Act, to respond to terrorist threats to Finland by freezing assets of several individuals. At the time of the on-site visit, the national list of such persons consisted of 7 individuals with links to Finland, and 38 from the EU list. Since its enactment in 2013, 14 persons and 8 entities have been subject to designations. However, although the elevated terrorism risk is quite recent in Finland (see IO.1), this number is low, particularly in light of the number of FTFs. It is estimated that around 80 Finnish residents have travelled to Syria to fight for ISIL, of which 30 have subsequently returned to Finland.

285. In addition, Finland has never made proposals for designation nor requested another country to give effect to its national freezing decisions and is not taking a proactive approach in that regard. Despite several national decisions to freeze assets, the Ministry of Foreign Affairs (MFA) has never informed the competent EU or UNSCR working group or committee about such a decision. The MFA did not provide reasons why the information had not been transmitted at EU or at UNSC level, and details of the national freezing decisions were not provided to the team. However, this reveals a relatively passive approach to designation. Finland - through its MFA - has only on one occasion co-supported with other EU members a proposal from a non-EU member for designation under UNSCR 1267/1988 and 1989.

286. Even though designation is not conditional upon the existence of a criminal investigation, LEAs use very seldom TFS when a criminal investigation cannot be initiated. This might be in particular relevant to address risks related to ISIL FTFs and returnees as suspected people may not be on Finnish territory. Obligated entities seem to effectively implement TFS (even though this cannot be confirmed by supervisors due to their lack of power in this field, see IO.3) and Finland benefits from an enforcement authority that ensures full and effective implementation. Implementation of asset freezes imposed at international and national levels is ensured by the Enforcement Authority. All natural and legal persons are required to freeze assets and funds of designated persons immediately. Financial institutions and DNFBPs implement this obligation to a large extent (see IO.4) and they immediately provide any information about accounts and amounts frozen to the Enforcement authority, i.e. the bailiff. The bailiff is also in charge of the identification of non-financial assets and has access to a wide range of information to ensure effective implementation. Assets frozen in relation to TFS amount only to EUR 10 600 belonging to three different persons (see below).

287. Obligated entities have a good understanding of their obligations on TFS as effective information and training is provided by the authorities. The NBI maintains a list of decisions to freeze funds which can be obtained from the local police departments or the NBI directly, upon request. The NBI's website provides information on the requirements of the Freezing Act as an example of the prevention

of terrorism financing. The MFA provides training to obliged entities and offers advice and support for the implementation of the TFS obligations, on an ad hoc basis. It has also issued guidance. Despite their lack of power in this field (see IO.3), supervisors do inform obliged entities of their TFS obligations. This is particularly the case for the financial supervisor FIN-FSA at the market entry level: it checks that relevant processes are in place to monitor sanctions lists, as part of the application for a financial institution licence.

Targeted approach, outreach and oversight of at-risk non-profit organisations

288. Even though Finland has a large and diverse Non-Governmental Organisation (NGO) sector (106 000 associations, 2 706 foundations, and 473 religious associations), Non-Profit Organisations (NPOs) that fall into the scope of the FATF Recommendations are more limited in numbers (around 1 000 associations and foundations have a valid money collection permit).⁶⁸ Associations and foundations are the most significant types of NPOs in Finland (see Chapter 1, Table 1.3).

289. Finland has identified a subset of NPOs at risk of TF abuse, but its analysis is not up-to-date. As part of the NRA 2015 (see IO.1), some stakeholders identified associations and in particular NPOs receiving state subsidies as at particular risk of TF abuse. However, this was not substantiated by analysis or cases. The 2009 report *“The financing of terrorism and Non-Profit Organisations”*⁶⁹ also identified a serious risk and significant growth potential in the abuse of immigrant-based associations. NPOs receiving state subsidies to provide aid to crisis areas were also identified as potentially at risk of TF abuse.

290. These findings about the subset of NPOs at risk were confirmed and developed further by the NBI in 2016. The FIU confirmed these findings on the basis of an analysis of STRs related to NPOs received between 2016 and 2018. Through these cases - which were disseminated to SUPO only - the FIU has identified around 50-60 NPOs at risk of TF abuse. They confirmed that NPOs operating in high-risk countries, having connections with individuals of interest to SUPO, using hawalas to transfer money to high-risk countries, and lacking transparency in the use of their funds were the most at risk of TF abuse.

291. As a result, LEAs as well as the FIU and SUPO, have a very good understanding of the risks related to NPOs. The assessment team has received classified reports, which demonstrate deeper understanding and important findings. A part of the knowledge is disseminated to some of the relevant authorities, including the National Police Board (NPB) which has some oversight responsibilities on some NPOs (see below), but only to a limited extent.

292. The level of awareness of the threat of abuse for TF purposes within the NPO sector is however moderate. It seems in particular that awareness in medium and small scale NPOs might be low. Large-scale NPOs seem to have processes in place,

⁶⁸ Non-Profit Organisations (NPOs) refer here to the definition of the FATF Glossary: *“legal person or arrangement or organisation that primarily engages in raising or disbursing funds for purposes such as charitable, religious, cultural, educational, social or fraternal purposes, or for the carrying out of other types of “good works”*.

⁶⁹ which involved the National Police Board, the National Bureau of Investigation, the Finnish Security Intelligence Service and prosecutors; see TC Annex, c. 8.1. a)

especially in their selection of partners, to prevent and detect any potential criminal abuse, in addition to the legal transparency requirements. Finland has not provided guidance, conducted outreach activities or developed focused actions vis-à-vis potentially vulnerable NPOs to prevent their possible misuse for TF purposes. Wider dissemination of the existing information on TF risks and threats would improve the overall understanding among relevant authorities and within the NPO sector.

4

293. Finland has effective general policies to promote accountability, integrity and public confidence in the administration and management of the NPO sector. The general registration, accounting and auditing requirements applicable to all NPOs, as well as the special NPB permit required for money collection and the associated reporting obligations (see Box 4.7, Chapter 1 and TC Annex, R. 8), are efficient measures to reduce the vulnerability of the segment of NPOs at TF risk. For example, the money collection permit process includes an evaluation of the applicant's operational mechanism in place for the appropriate use of the collected funds. Finland also has a range of legal provisions in place to protect NPOs receiving state subsidies from being abused by criminals, which are also relevant for CFT purposes.

Box 4.21. Money Collection Act and the prevention of TF abuse

As a rule, registered associations, religious communities and foundations may be given the right by the local police or the NPB, upon application, to organise money collections (Money Collections Act, Section 7). One of the conditions is that the NPO opens a bank account for the money collection (Money Collections Act, Section 17).

The NPB has general competence and responsibility for guidance and supervision in relation to money collection, including by those entities that have been given permits to conduct such activities and those that operate without licence, which are also part of the subset of NPOs at risk (see TC Annex, c. 8.1 and 2) (Money Collection Act, Section 26). The NPB may also file criminal complaints to the police in relation to money collection.

294. Finland conducts some oversight of the NPO sector, which is not a targeted and risk-based approach. The Money Collection Act (see Box 4.7) seeks to prevent dishonest activity in connection to money collection campaigns, including CFT. Preventing organised crime and TF is explicitly mentioned as one of the Act's objectives. When conducting the in-depth process to issue the money collection permit and when reviewing the money collection reports provided by NPOs, the NPB indicates that it takes into account ML/TF risks. However, the NPB was not able to demonstrate how this is done in practice, beyond having the intention to place special focus in 2018 on collections in which funds may be sent abroad, as well as on fund-raising campaigns permitting cash collection. NPB's money collection reviews follow established guidelines regarding collection profit, implementation costs and net profit. If any irregularity is detected, administrative proceedings can be initiated. The police can also be informed about possible illegal activity. This acts as a positive preventive and dissuasion tool.

295. In addition, authorities regularly raise public awareness – especially in times of humanitarian crises – about the required conditions to collect money legally. The

level of awareness of these obligations is very high in Finland and the authorities presented cases and examples of individuals reporting to authorities money collections conducted without permit. Some of these cases led to police investigations, but never for TF.

Deprivation of TF assets and instrumentalities

296. Finland uses TFS as a tool for depriving terrorist, terrorist groups and financiers of their funds and assets only to a very limited extent. Assets frozen in relation to TFS amount only to EUR 10 600 belonging to three different persons. Finland has made use of TFS to respond to terrorist threats to the country by freezing assets of several individuals but in very few occasions.

Consistency of measures with overall TF risk profile

297. The use of TFS against TF in Finland is not totally in line with the country's risk profile. In particular, Finland's most significant exposure to TF risks is through FTFs and returned fighters but the number of cases involving FTFs has been limited so far compared to the overall numbers of returnees in Finland (see above).

298. It is not clear that effective steps have been taken to freeze the assets of FTFs who remain in Syria, to prevent assets being transferred to them, or to prevent returned FTFs from providing financial support to terrorism. As noted above, Finland has exposure to terrorism and TF risks as a result of the 80 FTFs who have travelled from Finland to Syria and of the 30 who have returned to Finland.

Overall conclusion on IO.10

299. **Finland has achieved a moderate level of effectiveness for IO.10.**

Immediate Outcome 11 (PF financial sanctions)

300. Finland is an advanced manufacturing economy, which includes a number of high-technology industries and many companies producing military or dual-use goods. Although Finland has a high-level industry and quite significant nuclear power production, the related nuclear industry is rather limited. There are cross-border financial and trade flows with Iran and very limited commercial exchanges with the Democratic People's Republic of Korea (DPRK) (Table 4.2).

Table 4.20. Exports and Imports from Iran and DPRK in 2015 and 2016 (EUR)

		Iran	DPRK
2015	Exports	40 631 000	144 000
	Imports	2 340 000	0
2016	Exports	77 966 000	2 000
	Imports	1 858 000	4 000

Source : Statistics Finland

Implementation of targeted financial sanctions related to proliferation financing without delay

4

301. The implementation of targeted financial sanctions (TFS) for PF in Finland is based on the European legal framework (EC Regulation 2017/1509 for UNSCR 1718 concerning the DPRK and EC Regulation 267/2012 as amended by EC Regulation 2015/1861 and 1862 for UNSCR 2231 concerning Iran). These regulations apply freezing measures to a broad range of funds and property. Freezing obligations under European regulations are applicable to all natural persons and all legal persons within the EU, and take effect immediately on publication of the regulations in the EU's Official Journal. EU designations are published immediately in the consolidated financial sanctions database, and updates are available through subscription. In addition, updates are included in the sanctions newsletter issued by the Finnish Ministry of Foreign Affairs (MFA) and on MFA's website.

302. As noted in IO.10, even though Finland has legal provisions that would enable it to implement UNSCR obligations directly by decree (Act on the fulfilment of certain obligations of Finland as a Member of the United Nations and of the European Union, "Sanctions Act"), authorities do not use them in practice. They wait until the EU process is completed. Implementation without delay therefore remains an impediment to Finland's effectiveness, as explained below.

303. Mechanisms regarding Iran do not suffer from technical problems related to implementation "without delay". Since Regulation 267/2012 was issued in March 2012, there have been only two occasions when the UN added designations to the list (on 19 April 2012, and on 20 December 2012). In both cases, these individuals and entities had already been listed in the EU framework (see Regulation 1245/2011 of 1 December 2011, and Regulation 54/2012 of 23 January 2012), and subsequently incorporated into relevant Annexes of Regulation 267/2012. Delays in transposition have therefore not had any practical effect on either sanctions regime.

304. As regards the implementation of the Joint Comprehensive Plan of Action (JCPOA), immediately after the "implementation day" of 16 January 2016, the MFA received reports from financial institutions (FIs) on the release of funds belonging to de-listed entities in accordance with the updated EU regulation. Updated provisions were circulated to subscribers of MFA's sanctions newsletter on 17 January 2016 and MFA's website was updated accordingly. Well ahead of implementation day, Finland had provided outreach to relevant stakeholders. An event on the forthcoming changes was organised by the MFA in November 2015, and another outreach event at the MFA took place after the implementation day in February 2016.

305. For DPRK, despite recent improvements, there remains a problem with delays of up to several weeks in transposing the latest UN designations into EU Regulations. The UN added individuals and entities to the list four times between March 2012 and November 2015. On three other occasions, the designations by the UN (of 22 January 2013, 7 March 2013, and 28 July 2014) took approximately four, six, and ten weeks, respectively, to be incorporated into the EU framework.

306. As regards the additions to the UN list of sanctioned persons and entities after 2016, some uneven progress has been achieved in terms of transposition delays at EU level. Transposition delays have varied between three days (UNSCR 2270 (2016)), and 18 days (UNSCR 2397 (2017)), and nine days for UNSCR 2321

(2016), seven for UNSCR 2356 (2017), six for UNSCR 2371, five for UNSCR 2375 (2017) and 10 for 30 March 2018 additions to UNSCR 1718 (2006).

Identification of assets and funds held by designated persons/entities and prohibitions

307. No assets had been frozen at the time of the on-site visit, pursuant to UN designations related to PF. Prior to the implementation day for the JCPOA (16 January 2016), the amount of funds frozen pursuant to Iran-sanctions was EUR 2 542 878,05 (assets of 5 designated entities frozen by 2 FIs in Finland).

308. Equally, no funds have been frozen in relation to DPRK in Finland, as no relevant assets or properties were found in the country. Several authorities have been involved in the implementation of expanded DPRK sanctions since 2016. The Sanctions Co-ordination Working Group (see Chapter 1) has also discussed implications of new DPRK related UNSCRs in meetings in May 2016, April 2017 and May 2018. For example, in January 2017, the MFA requested the National Land Survey to search its registers for any DPRK owned real property, following UNSCR 2321 (2016), but none were found. Equally, and still in relation to UNSCR 2321 (2016), MFA conducted relevant researches regarding banking relationships of DPRK diplomats, in close co-operation with MFA's Protocol Services, Finnish Security Intelligence Service (SUPO) and Financial Supervisory Authority (FIN-FSA) and the European Commission (through a consolidated list of North Korean members of diplomatic missions in EU Member States) in view of ensuring compliance with restrictions targeted to diplomatic personnel of the DPRK.

309. Relevant authorities (MFA and SUPO) have demonstrated a good understanding of their obligations related to PF, export control and dual-use items.

310. Finland's export control authorities have a good understanding and coordination of duties related to PF, including from diversion and sanctions evasion and cooperate effectively to identify potential cases. The NBI and Customs which are responsible for the criminal investigation of proliferation, PF, and sanctions evasion have good operational co-operation with each other and with other relevant authorities, such as SUPO, MFA, and Enforcement Authorities. There is effective communication between export-control authorities and financial crime authorities in this regard. Customs are using a set of risks indicators which enable them to detect automatically dual goods exports or imports, and check manually afterwards with MFA, the police and SUPO, whether to investigate further on these cases. Information sharing and co-operation at the domestic level, and with international partners when necessary, is effective.

311. In practice, authorities have started a limited number of investigations which did not lead to prosecutions for PF. Most cases were closed by NBI based on a lack of grounds as there was no reason to suspect an offence for PF. Customs indicated that most of the time, investigations demonstrated that the activities were "regular" business and linked to transit documentation issues. The exporter or importer got permission to resume the operation afterwards. Finland is also mostly a country of transit for dual goods. Consequently, most of the time investigations relied on co-operation with foreign countries, where the initial offence had been committed and where the suspected offender was. Finland is contacting and cooperating proactively with its counterparts in such situations (see Box 4.8). Finally, effective preventive action and collaboration as well as active dissemination by the authorities of

information to the exposed companies also explain the limited number of investigations.

Box 4.22. Example of a criminal investigation conducted by Customs related to Proliferation

In 2011-2013, Finnish Customs conducted a criminal investigation of a suspected regulatory offence and a failure to file an export supervision report on dual use products.

A dual-use item had been exported by air to the United Arab Emirates (UAE) without the required export authorisation. The offence was suspected of having been committed in Finland in 2011. The Finnish Company X had sold the dual use item to Company Y. The buyer had informed Company X that the item was to be exported to Pakistan. Export to Pakistan would not have required an export authorisation.

In accordance with Annex I of the Council Regulation (EC) No 428/2009, export to UAE was not subject to authorisation. However, the MFA had notified Company X that an export authorisation would be required for the frequency converter in case the export destination was Iran or the UAE. Neither Company X nor the buyer or forwarder had applied for authorisation.

After the criminal investigation was completed, the case was submitted to the prosecutor for the consideration of charges. In the non-prosecution decision of 2013, the prosecutor determined that the acts committed did not constitute an offence. Only the exporter and the broker can commit a regulation offence or fail to file an export supervision report of dual use (Act on the Control of Exports of Dual-Use Goods, Sections 3, 4 and 9).

FIs and DNFBPs' understanding of and compliance with obligations

312. FIs and DNFBPs understand their obligations but have low awareness of common typologies of sanctions evasion. The MFA has produced guidance⁷⁰, organised seminars, and effectively provide on line assistance and advice to FIs and DNFBPs that have questions regarding their obligations. They have also organised more focused discussions and briefings to help small and medium enterprises, including small FIs and DNFBPs, to better understand their obligations on export control regimes and TFS. Lists of obligations are circulated to obliged entities on a regular basis, and outreach was done in advance of implementation of the JCPOA (see above). In addition, the MFA updates information provided on its website in an appropriate manner and has an email listing service. SUPO, FIN-FSA, and Customs

⁷⁰ MFA website – guidelines on dual-use items and export control
<http://formin.finland.fi/public/default.aspx?contentid=370971&nodeid=49544&contentlan=2&culture=en-US>

also contribute to these outreach activities. SUPO provides training and visits companies at risk of abuse for export of dual-use objects on a regular basis.

313. Even though conditions for compliance of FIs and DNFBPs with their TFS obligations are met, it is difficult to assess with certainty effective implementation as supervision is lacking in this field (see below on the lack of supervisory powers and IO.4).

314. Lists of designated persons and entities are available to financial institutions and DNFBPs through publication on the EU website, and are included in the consolidated lists used for automated screening purposes. Changes on TFS list are available immediately and the MFA provides an updated list to those who subscribe to an e-mail-listing service. FIs have confirmed that PF related sanctions are included in the lists used for real-time and periodic screening.

315. Although no assets have been frozen in practice with regards to Iran and DPRK TFS for PF (see above), the enforcement of freezing obligations is ensured in Finland by the Enforcement Authority. In 2017, all detected cases (35) were false positives but these cases have shown that there is an effective system in place to enforce the PF obligations. The Enforcement Authority (the bailiff) enforces the obligations, based on the freezing decisions by the NBI. FIs and DNFBPs immediately provide any information about accounts and amounts frozen to the Enforcement Authority. The bailiff is also in charge of identification of non-financial assets and has access to a wide range of information to ensure effective implementation. In practice, the Enforcement Authority and the MFA also help obliged entities to fulfil their obligations when there is a lack of essential identifying information.

Competent authorities ensuring and monitoring compliance

316. Supervisors do not have powers to supervise the implementation of TFS and therefore no sanctions for failure to implement TFS related to PF can be imposed on FIs and DNFBPs, which is a major weakness for the effectiveness of the regime against PF in Finland. Some supervisors -FIN-FSA and RSAA- do check in practice if the relevant screening processes are in place when conducting the license-granting process. They may also check when conducting an on-site visit with firms.

317. If there are suspicions of breaches of TFS on PF, FIN-FSA will report to the NBI as part of its general duty to report a breach of the law. The Sanction Act, together with the Criminal Code, provide for penalties and forfeitures for violations of EU Regulations (Regulation offence, Chapter 46 of the Criminal Code). However, as laid out earlier, authorities did not provide cases or court proceedings involving breaches of TFS obligations.

Overall conclusion on IO.11

318. **Finland has achieved a moderate level of effectiveness for IO.11.**

CHAPTER 5. PREVENTIVE MEASURES

Key Findings and Recommended Actions

Key Findings

- a) The understanding of ML/TF risks varies across financial institutions (FIs). Understanding of ML risks is more developed among larger FIs and those belonging to international groups. However, there is a risk that FIs belonging to international groups may focus more on group-wide risks without fully considering the specificities of the Finnish market. The understanding of some FIs, especially smaller entities or new market entrants is less mature and some may adopt a generic “tick box” approach to risk assessment. Understanding of TF risk is less developed across all sectors.
- b) FIs have implemented procedures to identify, assess, understand and document their risks. However, many FIs are on the first iteration of the process, and models are being further developed.
- c) Overall Designated Non-Financial Businesses and Professions (DNFBPs) are less aware than FIs of their ML/TF risks.
- d) Most DNFBP sectors have commenced risk assessments of their individual activities. Compliance knowledge currently available in these entities may not be adequate to mitigate their ML/TF risks. DNFBPs receive little guidance or supervisory support on implementation.
- e) FIs have implemented mitigation measures concerning customer due diligence (CDD), record keeping and monitoring, based on relevant risks. Larger FIs or those belonging to groups have more resources to devote to their systems or can avail themselves of group resources.
- f) FIs have an adequate understanding of, and screen for, specific high-risk situations that require enhanced measures, particularly in relation to politically exposed persons (PEPs) and higher risk countries. All demonstrate awareness of the appropriate escalation process when positive sanction hits are identified.
- g) DNFBPs generally apply CDD measures and take appropriate measures in higher risk situations including when dealing with foreign customers and PEPs. DNFBPs also avoid dealing in cash.
- h) Most DNFBPs face implementation challenges, and all experienced challenges with obtaining corporate information relating to foreigners and the beneficial ownership obligations.
- i) STR filing requirements are reasonably well understood by FIs. However, the number of STRs filed for some high risk FIs (for example hawala providers) and other sectors remains low to non-existent. There are concerns about the time delays and quality of reporting for some FIs.
- j) Overall the number of STRs reported by the DNFBP sectors is low, which is of serious concern, with the exception of reporting by gambling operators.
- k) The internal control policies and procedures in place appear adequate for FIs, and no obstacles have been identified with respect to information sharing within international financial groups.

- l) DNFBPs' application of internal controls and procedures is adequate in only a few sectors. Real estate agents and attorneys largely depend on industry association engagement and awareness material, rather than on engagement with the relevant supervisory authorities, RSAA and the Bar Association, respectively.

Recommended Actions

Finland should:

- a) Ensure that FIs and DNFBPs enhance their understanding of ML/TF risks, with a strong focus on TF risks across all sectors. Such actions should include the provision of practical ML/TF risk guidance to all sectors, with information on both ML and TF risk typologies, the most vulnerable sectors and red flag indicators.
- b) Ensure that FIs and DNFBPs enhance their ML/TF risk mitigation and control frameworks proportionate to their identified risks. Such actions should include the provision of guidance on the implementation of appropriate and proportionate AML/CFT measures to address identified risks. This guidance should be sector specific and with a particular focus on smaller FIs, non-banking sectors and DNFBPs.
- c) Raise awareness and ensure better quality STR reporting by FIs and DNFBPs. This should be supported by the intensification of supervisory focus and oversight of compliance with STR filing obligations and the timeliness of suspicious transaction reporting. Additionally liaison between supervisors and the FIU should be enhanced to facilitate
 - (i) targeting of reporting entities and sectors where weaknesses in suspicious transaction reporting have been identified and
 - (ii) sector-specific awareness-raising sessions with FIs and DNFBPs on understanding and applying the indicators of possible ML/TF suspicious activities, and timely reporting to the FIU.
- d) Ensure that FIs and DNFBPs' internal staff and managers responsible for ensuring compliance with the AML/CFT obligations, including compiling the ML/TF risk assessment, are adequately trained and knowledgeable, and seek assistance from sector industry associations and supervisors in that regard.

319. The relevant Immediate Outcome considered and assessed in this chapter is IO.4. The Recommendations relevant for the assessment of effectiveness under this section are R.9-23.

Immediate Outcome 4 (Preventive Measures)

320. Assessors' findings on IO.4 are based on interviews with a range of private sector representatives⁷¹, as well as the experience of supervisors and other

⁷¹ The financial institutions and DNFBPs met by assessors during the on-site visit included a selection of big and smaller banks which in total represent a significant share of the market in terms of the assets; two payment companies; a mutual life insurance company; an investment

competent authorities concerning the relative materiality and risks of each sector. The assessment team grouped the obliged sectors into categories in terms of their significance for the overall picture of compliance, see section on Financial Institutions and DNFBPs).

Understanding of ML/TF risks and AML/CFT obligations

Financial institutions (FIs)

321. FIs have an adequate understanding of their exposure to ML/TF risks. This understanding appears to be in line with the national picture of ML risks, however there are some gaps on the TF side. FIs have implemented processes and procedures to identify, assess and document these risks. Specifically, the understanding is more developed among larger institutions or those belonging to international groups. The banking and larger payment service providers' understanding is also better than those operating in the capital market and insurance sector. Smaller entities such as money remitters particularly those operating "hawala-type" money remittance and consumer credit providers, need most improvement.

322. Some FIs, and especially new market entrants may initially adopt a generic "tick box" approach to risk assessment. There is a risk that FIs belonging to international groups may focus more on group wide risks without fully considering the specificities of the Finnish market.

323. FIs indicate that risk assessment is conducted on an annual basis or more frequently if required, for example if new products or services come on line. However, while the legal requirement to adopt a risk-based model has been in force since 2008, many FIs entities are only on early iterations of the process, or still developing their models in this regard.

324. There were mixed views among FIs with regard to the continued relevance of the information included in the NRA 2015 (see IO.1), with many FIs considering it outdated or of little relevance to their operations. All FIs advise that TF is included as part of their risk assessment but would welcome more information from the FIU in relation to TF typologies and risks.

325. All FIs were aware of their obligations under the AML/CFT Act to conduct their own risk assessments, have appropriate AML/CFT frameworks and other preventive measures in place, and to file STRs.

DNFBPs

326. The level of understanding of DNFBPs of ML/TF risks and the mitigating control measures is adequate in some sectors (casinos and real estate, and then attorneys), but varies across remaining DNFBP sectors, and within sectors, due to size and complexity of the obliged entity business.

company; a money remittance company, an agent of a money remittance company and two hawala-type remittance firms; two crypto-currency service providers; three major real estate agents, as well as an Association of real estate agents; two major firms operating in the precious metals and stones sector, as well as the Finnish association of goldsmiths; a major law firm and the Finnish Bar Association; a major accounting firm; and both gambling operators.

327. The main ML/TF risk in DNFBPs' understanding is related to the use of cash in daily business activities. The exposure and handling of cash, as well as the use of pooled accounts, was identified as a high ML/TF risk across all DNFBP sectors in the NRA 2015. However, the current sense is that the prevalence of cash abuse and the use of client pooled accounts have diminished substantially.

328. Casinos, attorneys, accountants and real estate agents demonstrated an adequate understanding of their ML/TF risks regarding the use of cash in transactions, real estate transactions, exposure to corporate clients (particularly with foreign ownership), and customer fund accounts. Other DNFBPs demonstrated a lesser level of risk understanding.

329. Overall DNFBPs are less aware of sectoral AML/CFT risks than FIs, and this can be attributed to little practical guidance or support from supervisors. The main exception is casino operators, as explained below. Real estate agents and attorneys have benefited from awareness material provided by the Real Estate Agents Association and the Bar Association, including non-enforceable guidance, on the application of the new AML/CFT legislation. Otherwise, the compliance in the DNFBP sector is largely driven by the expectations of the banking sector and the fear of de-risking.

330. The two casino operators have a good understanding of the new obligations under the 2017 AML/CFT Act, with a practical, self-derived, understanding of ML/TF risks they face, and have each completed a risk assessment of their activities. However, the compliance resources currently available in these entities are not sufficient for them to fully comply with their obligations (e.g. filing reports to the FIU based on suspicious behaviours), and to mitigate their risks.

331. Real estate agents generally have a good understanding of their ML/TF risks and a sound and detailed understanding of their AML/CFT obligations. This is attributed mainly to the awareness work done by the real estate industry associations to real estate sector entities, who indicated that they turn largely to the industry association awareness material on the application of the AML/CFT legislation. The real estate associations have intermittent direct engagement with the RSAA, as supervisor. The real estate industry and their obliged entities are unable to learn from inspections conducted as these are few in number, and the inspection outcomes are not publicised. A number of real estate agents belong to financial groups, and benefit from the support and processes in place at the group level.

332. The Bar Association and attorneys have an understanding of the new obligations under the 2017 AML/CFT Act, and have generally commenced risk assessments of their activities. The level of understanding of ML/TF risks and AML/CFT obligations of independent legal professionals, who are not represented by any association, remains unknown.⁷²

333. Accountants have a basic understanding of the 2017 AML/CFT obligations, and appear to have an appreciation of ML risk in their activities; whereas dealers in precious metals and stones in jewellery and scrap metal have a very basic

⁷² The assessors were only able to interview major law firms, but did not interview representatives of independent legal professionals during the on-site.

understanding of the 2017 AML/CFT obligations, with few having commenced a risk assessment of their activities.

334. In the absence of comprehensive supervision of the DNFBPs, it cannot be concluded that entities across all sectors are aware of the obligations to conduct an individual assessment of ML/TF risks and to have in place risk-based procedures.

Application of risk mitigating measures

Financial institutions

335. Overall, FIs have implemented mitigation measures concerning CDD, record keeping and monitoring, based on relevant risks. Larger FIs or those belonging to groups have better measures in place than smaller ones.

336. FIs have determined risk mitigation measures for their identified risks and assessed the quality of their mitigation measures as part of the overall process. They make use of monitoring systems to assess the adequacy of controls to mitigate risks and take action to increase controls where higher inherent ML/TF risks are identified. FIs indicate that remediation programmes have been put in place where weaknesses are identified in controls. FIs with poorer understanding of the ML/TF risks related to their operation also had the weakest controls.

337. All FIs indicated that a higher level of initial and ongoing due diligence and transaction monitoring is implemented for those customers identified to be of a higher risk, for example corporate customers who operate in high-risk geographic zones, or cash-intensive businesses. Some FIs have several legacy systems used in CDD and ongoing monitoring of the customer relationship. The information is not transferred automatically between systems. In such instances, AML/CFT information on customers may not be available for all business areas and there is a risk that customers may not be categorised consistently and/or correctly across the institution.

338. The understanding and sophistication of implemented measures seem most developed in larger FIs or those belonging to (international) financial groups. For example initial and ongoing screening and transaction monitoring is generally automated (as opposed to manual) and conducted on a more frequent basis for such FIs. Additionally many such FIs have centralised their screening and monitoring at group level.

339. However, technical solutions to reduce manual work in risk management are still expensive for smaller FIs, and therefore not all supervised entities are using the best possible solutions. All FIs indicate that transactions would not be permitted where adequate CDD documentation has not been received.

340. FIs that rely on agent networks (such as money remittance providers and investment firms) indicate that they have implemented agent-oversight policies and procedures. Some larger money remitters have established systems to identify linked transactions which exceed CDD and reporting thresholds. Such systems also prohibit agents from undertaking transactions if CDD is incomplete or red flag indicators such as high-risk countries are raised. Notwithstanding this, it was noted that certain agents of EU money remitters' passporting into Finland do not appear to have access or oversight of monies passing through their individual agencies as this information is centrally held by the head office of the passporting firm.

DNFBPs

341. DNFBPs generally apply mitigation measures. However they are not fully commensurate to their risks. The obliged entities had little time to understand how they had to assess their ML/TF risks, be trained on the process, and then complete their initial risk assessment of ML/TF risks. Accordingly, obliged entities had little opportunity to put in place policies, procedures, and controls that are sufficient to reduce and effectively manage their identified risks of ML and TF.

342. Mainly, the risk mitigation measures consist of limiting the exposure of the DNFBPs to cash transactions. Attorneys and accountants rarely handle cash from clients, and where they do handle clients funds, they are required to hold these funds in a separate trust account for the client. They avoid using pooled accounts for their clients.

343. Real estate agents generally refuse to take cash; they hold only a maximum of 4% of the sale transaction value in a pooled bank account for their client; and they are paid their commission separately and out of the bank account where the deal is processed.

344. While dealers in precious metals and stones prefer not to deal in cash, high-end jewellery stores often deal in cash from tourist customers. However, the ML risks of such cash purchases are very low as it is not worthwhile for criminals to launder money through the purchase of jewellery items due to the substantial loss in value of these items on re-sale.

*Application of customer due diligence (CDD) and record-keeping requirements**Financial institutions*

345. *CDD Measures* - FIs generally apply adequate CDD measures to identify and verify their customers by using the electronic Bank ID for retail customers, Finnish social security numbers and the population register, as well as private credit agencies like *Suomen-Asiakastieto-Oy*, to identify and verify proof of address. For customers that are Finnish companies, in addition to declarations from the client, financial institutions rely on information contained in the companies register, although the register does not include information on beneficial owners and shareholders, which must be obtained from the company itself. Financial institutions indicate more difficulties obtaining beneficial ownership information for non-domestic companies but indicate that the proportion of such customers is very small when considered as part of the overall customer base.

346. *Ongoing Monitoring* - For monitoring purposes, FIs make use of different scenarios and rules in line with risks at the national level, which they include in their operations and transactions monitoring systems. The alert thresholds are more stringent for high-risk situations. Additional or different scenarios are also developed according to the risk level of the client. The sophistication of implemented measures is more developed in larger FIs belonging to larger financial groups.

347. *Record Keeping* - FIs have adequate record-keeping systems. Many indicate that they keep records for periods in excess of statutory obligations in this regard. All FIs are aware that they should refuse or terminate client relationships if the CDD process cannot be completed.

DNFBPs

348. *CDD Measures* - While DNFBPs do apply the CDD and record keeping measures, the actual implementation levels vary widely across and within sectors. Larger DNFBP entities and those associated with financial institution groups do better in this area, as they have the resources and skills to adequately meet these requirements. The level of application by smaller entities across all sectors is often basic, with compliance in these areas driven more by their expectations that the banking sector does the main compliance work, and a sense of concern about de-risking by banks.

349. Generally, DNFBPs have standardised their on-boarding measures and most use some form of customer application form to record the identification and other relevant information (address, occupation, etc.) about the client. On-boarding control measures are used to identify the risk profile of the client and whether enhanced due diligence may be required, such as when the client is a politically exposed person (PEP). In general gambling operators determine and apply CDD measures and other control measures (such as game addiction prevention) to mitigate various risks relating to whether the client is a resident or foreigner.

350. The extent to which business is refused, when CDD is incomplete, also varies, with a stricter approach applied by larger DNFBPs and those related to FIs. In contrast, smaller and more retail-focused DNFBPs are inclined to accept the business for profit-driven reasons. A few indicated they may then consider filing a report to the FIU.

351. *Record keeping* - Obligated entities confirmed that they keep client records for the prescribed period. Most DNFBPs (attorneys, accountants and real estate agents) and the larger obliged entities appear to have adequate record keeping measures in place. The remainder of DNFBPs and smaller obliged entities appear to have basic record keeping procedures in place consistent with their type of business and record keeping processes ordinarily applied in their day-to-day operations.

352. The low number of inspections across the various sectors has not assisted in demonstrating the full effectiveness of record keeping measures. The 2017 RSAA supervisory findings identified record keeping deficiencies in four of 10 inspections of real estate agents. The state of adherence to CDD measures and the record keeping requirements amongst obliged entities has not been regularly monitored or assessed by competent supervisory authorities.

Application of enhanced due diligence (EDD) measures

353. FIs have implemented adequate risk-based mitigation measures concerning enhanced or specific CDD, record keeping and monitoring. In general, they tend to take a cautious approach to any situation presenting potential higher risks and take appropriate, enhanced measures to manage and mitigate those risks. DNFBPs have a more uniform approach when applying CDD measures and seldom apply differentiated sets of CDD rules to their customers, based on risks, except when PEPs are identified.

Financial institutions

354. FIs have implemented adequate risk-based mitigation measures concerning enhanced or specific CDD, record keeping and monitoring. However, supervisory authorities indicate that the quality of applied EDD procedures can vary between supervised entities.

355. *Correspondent Banking* - FIs indicate that the number of correspondent banking relationships has generally declined in the period under review. Many FIs have exited such relationships in higher risk countries. All FIs who have correspondent banking relationships advised that they complete initial due diligence and ongoing monitoring of such relationships, including the additional measures required by the AML/CFT Act which only extend to relationships with entities based in non-EEA countries (see TC Annex, R. 13).

356. *PEPs* - The frequency of PEP screening varies between FIs. Depending on the sophistication and automation of the screening system used, screening of PEPs can vary from daily to periodic screening over the course of a year. Again, this is because the pricing of automated screening systems can be prohibitive for smaller or stand-alone entities. Notwithstanding this, all FIs advise regular and enhanced ongoing monitoring of PEPs.

357. *Targeted financial sanctions (TFS) and higher risk countries identified by the FATF* - There is uncertainty regarding the level of compliance by obliged entities with regard to TFS for TF, since supervisors lack powers to supervise the implementation (see IO.3). FIs frequently utilise commercial providers in complying with financial sanction regulations concerning CFT and CPF and limitations applying to high-risk countries. As a result, the monitoring of sanction lists (international financial sanctions regimes and domestic listings of freezing of funds to prevent terrorism) and customer relationships concerning high-risk countries has been automated to a large degree. However, the cost of real-time monitoring of sanction lists has proven prohibitive for some small supervised entities due to the pricing of the commercial services. Such firms have to resort to a manual screening process, which by its nature is not real time, and as such not as effective as automated screening. All FIs demonstrated awareness of the appropriate escalation process to the external authorities when positive sanction hits are identified.

358. *Higher Risk Customers* - Many FIs consider non-resident customers (both natural and legal persons) as higher risk, and they indicate that they have exited customer relationships or will not accept customers from higher risk jurisdictions in this regard. They also indicate that they will not on-board customers or have exited customer relationships for sectors that they perceive as being of higher risk. Such customers include “hawala-type” money remitters and crypto currency issuers and exchanges. This has caused difficulties (particularly access to banking facilities) for many regulated FIs perceived to be of higher risk (e.g. hawala providers) and such firms have indicated that it may result in the closure of their businesses. There is a risk that the unregulated or underground service providers may flourish in such circumstances.

359. *New Technologies* - FIs indicate that the development of new products and services, including those involving new technologies, are subject to AML/CFT analysis and advice from the compliance department is a mandatory part of the

product approval process for FIs. The identification and consideration of the risks associated with new technologies such as on-line services, e-money and prepaid cards also forms part of FI's risk assessment process.

DNFBPs

360. EDD measures are generally not applied outside of DNFBPs associated with financial groups, and most DNFBs are waiting on government decrees to be issued (see TC Annex, R. 1 and 10) or supervisory authority announcements to spell out the detail of how best to apply EDD measures in particular circumstances. Most DNFBP associations and obliged entities advised that there is insufficient guidance by the policymaking authorities, and applicable designated supervisors on the application of EDD measures. In the absence of supervisory guidance, which could assist entities to develop and apply a common understanding of the compliance requirements, it cannot be said that EDD measures are being applied consistently based on a common understanding across sectors. The EDD measures that are applied relate to PEP identification and verification of identity and non-face-to-face identification. Most obliged entities use a standard client application form in which they require the prospective clients to disclose whether they are a PEP or not, or are related to or have some association with a PEP.

Reporting obligations and tipping off

361. There is a good level and quality of reporting by the FIs, particularly from the banking sector. TF reporting is more limited and of lower quality, mainly due to the lack of TF knowledge. For some higher risk FIs, and in particular hawala-type money remitters, the level of reporting is insufficient. Regarding DNFBPs, with the exception of the gaming sector, the reporting of suspicious activity occurs at very low levels. While the low number of STRs may be explained by a low level of cash transactions, the assessors are unable to reach conclusion on the adequacy of the reporting since Finnish authorities have not provided their own analysis of this reporting.

Financial institutions

362. The suspicious transaction reporting (STR) filing requirements are reasonably well understood, however, there are concerns about the time delays and quality of reporting for some FIs.

363. The number of STRs filed by each type of FI is presented in Table 5.1. Most FIs interviewed indicate that they file STRs within two to four weeks of initial transaction/suspicion and always immediately if the suspicion is deemed high priority (such as the opportunity to freeze money). However, some FIs advise considerable backlogs (several months) in reporting non-priority STRs to the FIU. Hawala-type money remitters (which are high risk) have not submitted any STRs in 2015-2017.

Table 5.21.: STRs reported by Financial Institutions 2015 to 2017 by Sector

Sector	No. FIs	2015	2016	2017
Money transfer services	4			
STRs		887	864	883
Threshold reports ⁷³		3368	3229	4009
Credit and financial institutions(banks) ⁷⁴	22	1 608	3 318	5 178
Insurance companies or pension insurance companies	27	33	40	57
Credit and financial institutions (other than banks)	10	19	82	123
Investment service providers	12	1	2	4
Foreign credit and financial institution branches	4	6	2	2
Funds management companies or depository corporations	2	2	1	0
Asset management and company service providers	1	0	0	0
Companies or co-operatives involved in limited credit institution business	2	0	0	0
Foreign investment service providers	1	1	0	5
Total	95			

Source: FIU

364. The quality of STRs can vary according to the FIU, and as observed by the FIN-FSA in their supervisory activities. Bigger banks provide higher quality reports. STRs submitted by smaller reporting entities are of less value to the FIU. Most of the STRs (around 99%) are submitted electronically through a web application (provided by the GoAML system used by the FIU, see IO.6).

365. While some of the larger institutions have met with the FIU in the last year to discuss STR filing, the discussion focused largely on the numbers of STRs submitted in comparison to peers. This is not adequate and most FIs would welcome increased feedback from the FIU on the quality of STRs submitted.

366. Most FIs indicated they have difficulty in detecting suspicious transactions related to TF, and again would welcome additional guidance from the FIU in this area. The FIU confirmed that the quality of reports related to TF is generally lower than for ML. Some reports submitted as TF-related are subsequently re-qualified by the FIU staff as non-TF, and vice versa. This is often due to the lack of the specific knowledge of TF suspects by the private sector.

367. The FIs acknowledge challenges with regard to tipping off in particular the possibility of alerting the relevant customer if the FI needs to ask further questions about a possibly suspicious transaction, but all point to internal escalation procedures and contact with the FIU as mitigation measures.

⁷³ See more information on the nature of Threshold reports in IO6.

⁷⁴ Credit and financial institutions (banks) may register one suspicious transaction in an STR as an example or many transactions which are not all necessarily suspicious. Thus, the volumes and values of incoming and outgoing transactions can be taken as indicative only.

DNFBPs

368. The reporting of suspicious activity occurs at very low levels across most DNFBP sectors (see Table 5.2). The only exception is the gaming sector which provided most of the STRs from DNFBPs. Their reporting indicates levels of suspicious activities that are cash based, also occurring online, and aboard leisure ships operating in the Baltic Sea. Importantly, the gaming service providers submit reports to the FIU on the basis of a set of criteria (risk indicators and monetary thresholds) discussed with the FIU. Due to the differences in the types of gaming service providers and the criteria for reporting (of which the amount of cash transaction is a key element), gaming service providers report differently STRs and threshold reports, although a total number of STRs and threshold reports combined in broad figures are comparable between these service providers. While the assessors did not receive any further information with regard to the nature of these criteria, they are of the opinion that the high levels of reporting by the gaming service providers is a direct result of the active engagement between the FIU and the gaming service providers. Accordingly, a programme of active engagement by the FIU with the remaining DNFBP sectors should increase reporting levels in those sectors.

Table 5.22. STRs reported by DNFBPs 2015 to 2017 by Sector

	2015	2016	2017
Gaming service provider (mainland and Åland)			
STRs	2534	1730	1787
Threshold reports⁷⁵	6809	10261	6635
Dealers in precious metals and stones	0	0	0
Attorneys and independent legal services providers	5	7	8
Real estate agents	8	11	11
Accountants	5	2	2

Source: FIU

369. The Finnish authorities were unable to explain whether the low number of reports in other sectors is adequate and what is driving reporting behaviour. This is due to the lack of supervisory engagement, poor knowledge of the supervised population and the absence of direct FIU engagement on reporting in these other sectors. While the low number of STRs may be explained by a low level of cash transactions, the assessors are unable to reach conclusion on the adequacy of the reporting.

370. DNFBPs are generally aware and understand the obligations relating to “tipping off” a client in respect of whom an STR has been filed. Most DNFBPs have trained staff on such matters.

Internal controls and legal/regulatory requirements impeding implementation

⁷⁵ See more information on the nature of Threshold reports in IO6.

Financial institutions

371. The FIs have adequate internal controls and procedures for AML/CFT compliance. FIs generally understand the importance and special characteristics of ML/TF risk and the importance of implementing an adequate associated AML/CFT governance and control framework (internal policies, procedures and controls) to mitigate such risks.

372. No FI raised obstacles with respect to the sharing of information within an international group. FIs belonging to international groups have implemented group-wide policies and procedures.

373. FIN-FSA has indicated that although FIs have increased their AML/CFT compliance personnel during the last five years, there have been challenges in building and organising robust compliance activities focusing on material issues. Finding a balance in resourcing and the expertise of personnel between the different lines of defence has proven to be a key question to be resolved by FIs at times.

374. All FIs indicated that they have compliance programmes in place and are subject to internal audits. They also provide targeted AML/CFT training to employees. As noted previously, the understanding and sophistication of implemented measures seem most developed in larger institutions belonging to (international) financial groups, and less in smaller institutions.

375. Some FIs highlighted apparent conflicting obligations between data protection requirements, AML/CFT obligations and the associated filing of STRs.

DNFBPs

376. DNFBP's application of internal controls and procedures is adequate in only a few sectors: real estate agencies that belong to banking groups, attorneys, and casino operators. These sectors have better access to specialist compliance capacity due to the industry guidance or group wide internal control programs. Casino operators have comprehensive internal controls and procedures in place and ensure their staff and agents are knowledgeable in applying these in gaming operations. While dealers of precious metals advised they had internal controls in place, it cannot be assumed that all obliged entities in this sector have implemented internal AML/CFT controls, and this is a major concern to be tested by appropriate supervisory action.

Overall conclusion on IO.4

377. **Finland has achieved a moderate level of effectiveness for IO.4.**

CHAPTER 6. SUPERVISION

Key Findings and Recommended Actions

Key Findings

- a) A number of FIs and DNFBPs are not required to register with the relevant supervisory authority, which renders their supervision very difficult. The obligation to register only enters into force on 1 July 2019.
- b) The FI supervisors apply reasonable fit and proper assessments to prevent criminals or their associates from entering the market.
- c) Appropriate fit and proper assessments are applied to only some of the DNFBP sectors at the market entry stage, mainly to real estate agents, gaming operators and attorneys.
- d) The FI supervisors' understanding of ML/TF risks is not adequate for the majority of sectors under their supervision. The identification and understanding of the ML/TF risks specific to the sectors and FIs they supervise is more substantial for the FIs with which they have ongoing supervisory engagement. However, this represents very few sectors within the overall population under their supervision (see Key Finding (f) below). Both FI supervisors are only in early stages of developing their risk assessment methodology.
- e) Amongst DNFBP supervisors, the RSAA's understanding of risk is most developed and more so with regard to the sectors with which it has more engagement. While the DNFBP supervisors (except the RSAA) have conducted a form of supervisory sectoral ML/TF risk assessments, these have not been fully aligned with the national view of risks.
- f) Overall, the supervision is not performed on a risk-sensitive basis. The FI supervisors concentrate their AML/CFT supervision on only those firms they view as being the very highest risk. This is of serious concern, particularly in the FI sector. FIN-FSA concentrates its supervisory efforts on the three largest banks. However, a number of other FI sectors are considered to represent higher risk, for example, hawala-type and other money remitters where there is limited to non-existent ongoing supervision. There is no supervision of lower risk firms.
- g) The FI supervisors have a range of remedial sanctions available. However, no penalties, fines or other sanctions have been imposed on FIs to date.
- h) The AML/CFT teams within both FI supervisors, as well as RSAA as DNFBP supervisor, are significantly under-resourced given the breadth and depth of their AML/CFT responsibilities and associated workload.
- i) No DNFBP supervisor is yet able to conduct adequate and robust AML/CFT supervisory engagement. Although most supervisors subscribe to a risk-based approach to supervision, they are still working through the modalities of how to do so.
- j) Some DNFBP supervisors have conducted few if any inspections in certain sectors. While inspections of obliged entities have begun, although in low numbers, the supervisors have yet to commence inspections in a

- systematic risk based fashion.
- k) No penalties, fines or other sanctions have been imposed by the DNFBP supervisors.
 - l) Supervisors lack powers to supervise the implementation of TFS although they do check that the necessary processes are in place when conducting the licence granting process.
 - m) FI supervisors provide guidance to FIs through different channels (e.g. website, newsletters etc), but in a limited manner. FIs have expressed a need for further guidance, particularly with regard to AML/CFT implementation issues and the identification of TF issues.
 - n) Little to no guidance has been provided to DNFBPs focusing on the AML/CFT risks to which the various industries/businesses/products are exposed.
 - o) The coordination amongst supervisors, and among supervisors and the FIU, to improve understanding and develop a common approach to attain effective AML/CFT supervision, as well as improve reporting by obliged entities, is not effective, with little regular communication and information sharing outside the FIN-FSA and the FIU.

Recommended Actions

Finland should:

- a) Require that supervisors improve their understanding of ML/TF risks by continuing to develop and adopt a relevant methodology and process. Formal sector-specific risk assessments should be undertaken, in particular with regard to hawala-type and other money remitters and legal professionals in relation to company formation. Their summaries should be published and appropriate actions taken to raise awareness around them. The outputs should clearly prioritise FI and DNFBP sectors for supervisory oversight and engagement.
- b) Require that supervisors, as a matter of priority, develop, adopt and implement a risk-based AML/CFT supervisory engagement model that takes into account the differing levels of ML/TF risks associated with individual FIs or DNFBPs and also each of the sectors supervised. Given the high level ML/TF risk attached to hawala-type money remitters, the engagement model should ensure these institutions are supervised on an ongoing manner appropriate to their risks. Finland should also ensure that the Finnish authorities take appropriate follow-up actions against unauthorised hawala-type money remitters and other unauthorised service providers.
- c) Ensure that the supervisors collectively and individually issue structured and practical guidance to obliged entities on the ML/TF risks, the risk assessment process, the interpretation of, and complying with, the AML/CFT requirements.
- d) Grant supervisory powers to all supervisors and Self-Regulatory Bodies of obliged entities for the supervision of the implementation of TFS for TF.
- e) Ensure that FIN-FSA and the RSAA take sanctions where appropriate against FIs and DNFBPs that do not comply with their AML/CFT

requirements. Such sanctions should reflect the severity of findings encountered.

- f) Substantially increase the supervisory resources of all supervisors in order for them to be sufficiently equipped to adequately and effectively adopt and implement a risk-based approach to supervision of the sectors that come under their remit.
- g) Operationalise the recently established AML/CFT Co-ordination Group to promote regular co-ordination of effort amongst supervisors, and between supervisors and the FIU, to improve understanding and develop a common approach to attain effective AML/CFT supervision, as well as improve reporting by obliged entities.
- h) Consider activating the ML register immediately, notwithstanding the legal effective date of July 2019, and permitting DNFBPs to commence registering voluntarily, as a means to confirm entity acknowledgement of their AML/CFT obligations, and to provide the RSAA with a growing sense of identifiable obliged entities with whom to reach out and engage.

378. The relevant Immediate Outcome considered and assessed in this chapter is IO.3. The Recommendations relevant for the assessment of effectiveness under this section are R.14, R. 26-28, R.34, and R.35.

Immediate Outcome 3 (Supervision)

Licensing, registration and controls preventing criminals and associates from entering the market

379. A number of FIs (providing services like corporate loans, financial leasing) and DNFBPs (high-value goods dealers and legal service offices) are not under a legal requirement to register (see Chapter 1). Although the RSAA has the statutory responsibility of AML/CFT supervision of these FIs and DNFBPs, it is uncertain of the exact numbers of obliged entities in the various sectors under its remit. This does drastically impede its effectiveness as a competent supervisory authority. This uncertainty has a direct effect on whether it is appropriately and adequately capacitated and financially resourced to adequately perform its supervisory functions. It also further impacts all supervisory planning and actions it may conduct. The RSAA points out that the transitional provisions for the establishment of a ML register in which obliged entities are to register with effect 1 July 2019, would hopefully assist in bringing certainty of the total universe of obliged entities under its supervision.

Financial institutions

380. Both financial supervisors (see Chapter 1, Table 1.1) apply adequate fit and proper assessments to prevent criminals or their associates from entering into the market. They also both take measures to prevent and detect unauthorised financial activities in the market. However, there is insufficient proactive action taken by Finnish authorities with regard to unauthorised hawala institutions, which are high-risk for TF.

381. Under the Single Supervisory Mechanism (SSM) (see Chapter 1), the European Central Bank (ECB) grants authorisations to Finnish banks based on their application submitted to FIN-FSA. With regard to ongoing fit and proper tests (F&P), final decisions are made through SSM *i)* for members of the management board and supervisory board of three Finnish Significant Institutions (SI)⁷⁶ and *ii)* for qualifying shareholders of all banks. Similar to authorisations, FIN-FSA conducts the initial F&P reviews and the ECB has the ultimate decision making power. The FIN-FSA remains responsible for approving members of the management board and supervisory board of Less Significant Institutions (LSIs) post authorisation.

382. FIN-FSA is also the assessor and final decision maker with regard to authorisation or registration, supervision, and F&P matters for all other FIs under its remit (i.e. life insurance entities, investment firms, payment institutions and money remitters, see Table 1.1). FIN-FSA applies F&P assessment of qualifying shareholdings, members of the Board of Directors, CEO and senior management before granting authorisation. FIN-FSA also conducts F&P checks on an ongoing basis with regard to changes to qualifying shareholdings, members of the Board of Directors, CEO and senior management. This is done using information from the criminal and fine register entries, credit record inquiries, as well as FIN-FSA internal information. In the period 2014/17, during ongoing supervision, a person was found for whom a F&P notification should have been made.

383. FIN-FSA advises that non-Finnish applications are predominantly from the EEA. In those cases, relevant information is provided through contacts with the competent authority of the country of origin.

384. In 2014-2017, FIN-FSA took specific actions at the stage of F&P process in three instances: removing an insurance broker from the register of insurance intermediaries, forbidding a person from acting in the management of an investment company and owning a share in the investment company, and rejecting an application to act as an investment firm. FIN-FSA has not imposed any F&P sanctions so far. During 2014-2017, one F&P case was referred to the sanction process. However due to technical legislative reasons, there were not legal provisions (principle of conforming to law) which permitted the commencement of the sanction process.

385. The RSAA carries out F&P checks on all FIs under its remit (e.g. consumer credits providers, financial leasing entities, currency exchange services, see Chapter 1, Table 1.1) applying for registration⁷⁷, as well as on changes in management and ownership post authorisation as notified by the FIs. The RSAA also proactively checks criminal records and trade registers on a periodic basis post authorisation and follows up with FIs if the required notifications have not taken place. The frequency of such follow up F&P checks are adequate in the view of assessors.

⁷⁶ Kuntarahoitus Oyj, Nordea Bank AB (publ), Finnish Branch, OP osuuskunta www.bankingsupervision.europa.eu/ecb/pub/pdf/ssm.list_of_supervised_entities_201802_en.pdf

⁷⁷ In the period between June 2017 and June 2018, currency exchange service providers and companies providing other financial services (e.g. non-consumer loans, financial leasing), were not *de jure* subject to registration or licensing requirements, however, this has not had major impact on the system.

386. To date the RSAA has not taken any supervisory sanctions against firms for non-notification of changes to ownership or management. While the RSAA claims that its follow-up with FIs is usually enough for such companies to submit their notification and no further official supervisory measures are needed, there is a danger that the effectiveness of this supervisory approach could be undermined in absence of a credible and enforced sanction regime to follow through with FIs on non-notification of such changes. Sanctions are discussed further in 6.2.4 below.

Table 6.23. F&P checks undertaken by the RSAA

	Consumer credit providers (and P2P mediators since 2017)			Currency exchange			TCSPs		
	2015	2016	2017	2015	2016	2017	2015	2016	2017
Number of new applications	11	11	12	2	6	4	2	8	5
Changes (new management etc.)	29	21	18	1	1	3	0	7	4
Denied applications	1	0	0	0	0	0	0	0	0
F&P checks (excluding new applications)	n/a	142	1	0	18	31	0	127	101
Actions based on F&P checks	0	1	1	0	0	0	0	1	0

Source : RSAA

387. FIN-FSA investigates potential cases of unauthorised Finnish or EU/EEA service providers operating in Finland and carries out formal follow-up actions vis-à-vis firms suspected of unauthorised activities (see Box 6.1). If the firm fails to comply with FIN-FSA's request within the deadline, FIN-FSA may refer the matter to the police for investigation. In the years 2014-2017, the FIN-FSA has made two requests for investigation to the police⁷⁸. In addition, one person was fined for the provision of unauthorised services in 2012. The FIN-FSA also issues warnings regarding unauthorised service providers from outside the EU/EEA, mostly regarding investment frauds.

Table 6.24. Unauthorised Service Providers Detected by FIN-FSA 2014 – 2017

Year	Credit Institutions	Insurance Companies	Investment Firms, Fund Activities etc	Payment Services	Insurance Intermediaries	Total
2017	1	3	5	4	0	13
2016	2	1	4	13	3	23
2015	0	1	0	0	0	1
2014	2	0	0	0	0	2
Total	5	5	9	17	3	39

Source: FIN-FSA

388. A number of hawala-type institutions successfully went through the authorisation process to become payment service providers once the legal requirement came into force in 2010. The FIN-FSA mentioned that during

⁷⁸ Case 1 in 2014: The Prosecutor made the decision not to prosecute. Case 2 in 2017: Still under consideration by the Prosecutor

2016/2017 nine hawala-type institutions failed to fill the required conditions and therefore were not granted the required registration. However, no follow-up actions have been taken by Finnish authorities to check if those institutions were still providing (unauthorised) services. This is a concern given that those entities are at high-risk, especially for TF. In 2016, the FIU conducted a hawala strategic analysis project (see IO.6), and identified some unauthorised hawala-type institutions. The FIN-FSA was informed and sent warning letters to 13 institutions. No further action was taken by Finnish authorities in this regard.

Box 6.23. Case Study: Unauthorised Activity

The case was initiated based on information provided by an authorised entity. FIN-FSA sent a letter to the institution to obtain more detailed information on its activities. On reviewing the response, FIN-FSA concluded that the institution should apply for authorisation, which it duly did. After discussions in relation to the authorisation, the institution decided to change its business model (which initially was an alternative investment manager). FIN-FSA concluded that the institution did not require authorisation after the changes in its business model.

389. The RSAA conducts periodic searches (usually once a year) of the Finnish Trade Register to ensure that FIs required to register with the RSAA have done so (e.g. currency exchange services which in some cases are provided by entities not aware that they need to be registered). The RSAA has taken supervisory measures against FIs for not registering as required. For instance, in 2015 the RSAA prohibited two companies from providing consumer credits without registration and the prohibition was enforced with a notice of conditional fine.

Box 6.24. Case Study: Detection of an unauthorised Service Provider by the RSAA

Initiated by customer complaints, in 2016, the RSAA detected an unregistered company providing consumer credit services online. To determine the actual nature of the financial services provided, the RSAA sent a request for information to the company. The request never reached the company due to lack of up-to-date contact information. Ownership of the company could be traced abroad. Unable to get in touch, the RSAA could not confirm whether the company's actions were legal or not. As a result, a request for investigation was made to the local police in 2017 to investigate whether the company was violating the penal provisions of the Act on the Registration of Certain Credit Providers and Credit Intermediaries (section 19). The investigation is ongoing.

DNFBPs

390. Appropriate F&P assessments are applied to some DNFBPs, mainly those under the remit of the RSAA (see Chapter 1, Table 1.1), gaming operators and attorneys. For the other DNFBP sectors, the licensing, registration and controls are substantially less or non-existent. The RSAA and the National Police Board/Gambling Administration (NPB/GA) have been proactive in the detection for some unauthorised activities, but this is not the case for other DNFBP supervisors.

391. Finland has a good system of licensing and entry requirements (involving some form of F&P market entry requirements) for some DNFBPs, such as the gaming operators and service providers like attorneys, and real estate agents. Given that legitimate gambling activities in mainland Finland and the autonomous region of Åland are exclusively conducted by two wholly government-owned corporations, there is a lower risk of infiltration or ownership of these entities by organised criminal groups or their associates. Accordingly, criminals are prevented from entering the gambling market or from being actual beneficiaries of a company running legitimate gambling activities in Finland.

392. Attorneys' F&P checks are conducted as part of the process to access the Bar. There are integrity requirements, which are duly checked by the Bar when reviewing applications, including good reputation as an honest person, which is cross-checked through a number of references, and not being bankrupt. For real estate agents, the RSAA applies the same approach as it does to FIs (see above), which is satisfactory.

393. For the other DNFBP sectors, the licensing, registration and market entry controls are substantially less (for accountants,) or non-existent (for independent providers of legal services, and dealers in precious metals and stones). This results in the remaining risk that criminals or their associates may enter the market and may own a company conducting these activities. In particular, there are approximately 840 offices providing independent legal services employing around 1 500 persons (estimated), which constitutes a significant vulnerability for abuse by criminals given the absence of market entry requirements.

394. The RSAA conducts some activities to detect unauthorised activities. Real estate is one of the sectors targeted and since 2015, the RSAA has identified five unauthorised real estate agents who were invited to regularise their situation, but no sanctions were applied.

*Supervisors' understanding and identification of ML/TF risks**Financial institutions*

395. FIN- FSA has not conducted a ML/TF risk assessment. Therefore, its understanding of the ML/TF risk and how its sectors fit into the overall risk landscape is not comprehensive. The RSAA has conducted sectoral assessments (though no firm specific assessments), and as such its understanding of risk is generally acceptable for the FI sectors it supervises. The level of knowledge and understanding of both supervisors is more advanced for ML risks than TF risks.

396. FIN-FSA has produced a document outlining at a very high level, the most significant generic ML/TF risks it perceives to exist within the general population of

FIs it supervises. However, this document is general in nature and does not provide any ML/TF risk assessment or ML/TF grading of specific sectors or the FIs it supervises.

397. In the absence of a specific ML/TF risk assessment, FIN-FSA's general view of a FI's riskiness is based on its size when viewed by market share, the breadth of its services offering, particularly those provided internationally, and its level of cash services to the extent it can be ascertained from direct engagements and/or prudential returns. However, there is no methodology or systematic review employed by FIN-FSA in its consideration of such factors. In addition, it has not undertaken this exercise for the majority of FIs or sectors under its supervision and this approach does not take into account ML/TF risks specific to the Finnish context.

398. FIN-FSA's identification and understanding of ML/TF risks specific to the sectors and FIs it supervises is significantly higher for the FIs with which it has ongoing ML/TF engagement. In particular, its understanding of the ML/TF risks related to the three largest banks is broadly in line with national ML/TF risks. Its interaction with foreign AML/CFT supervisors of these cross-border FIs, especially those in the Nordic region, is an important source of information in this regard. However, it is essential for FIN-FSA to also look inward at the ML/TF risks faced by these FIs in the Finnish ML/TF context, taking into account the national specificities and characteristics (see IO.1). For other FIs and sectors, its understanding of the ML/TF risks is more academic in nature and is based on its perceptions of where ML/TF risks may arise as opposed to being grounded in actual supervisory experience and knowledge of the current and/or emerging ML/TF risks specific to the FIs.

399. FIN-FSA has taken initial steps to gather information with a view to commencing its ML/TF risk assessment. In this regard, it has issued tailored questionnaires to 17 banks and it intends to roll out tailored questionnaires to other sectors later in 2018. FIN-FSA has also commenced a project to create an IT tool to collate, analyse and risk rate ML/TF data from a number of sources including these questionnaires. All these measures are only in the initial stage, and have not yet contributed to a comprehensive understanding of ML/TF risks.

400. The RSAA commenced its risk assessment process in 2014, produced its first assessment in 2015 and has updated it on an annual basis thereafter. While the risk assessment appears to be broadly in line with the services offered by the sectors under its remit, it is predominantly qualitative in nature. The RSAA has utilised to a limited extent, questionnaires issued to consumer credit providers and currency exchange services to gather additional information to inform its views. However, overall, the risk assessment lacks substantive quantitative input to support its findings.

401. The RSAA's understanding of risk is most developed with regard to the sectors with which it has had the most engagement so far, for example currency exchange providers. The RSAA is currently in the process of refining its risk assessment and developing a methodology to apply risk ratings on a firm-by-firm basis.

Table 6.25. ML/TF risk score rating of FI sectors supervised by RSAA (2018)

ML/TF Risk Score	Type of Obligated Entity
3 – significant risk	Currency exchange businesses
2 – medium risk	Consumer credit providers Other creditors and financial service providers (corporate loans, etc.)
1 – low risk	Holders of debt collection permits
The risk level is defined on a scale of 1-4 (1 = low risk, 2 = medium risk, 3 = significant risk, 4 = very significant risk).	

Source: RSAA

DNFBPs

402. The understanding and identification of ML/TF risks vary in level of detail and scope amongst the DNFBP supervisors. The RSAA, the NPB/GA, and the Bar Association generally exhibited a good level of understanding of the ML/TF risks present in their respective sectors, which they, *inter alia*, contextualised based on the findings of the NRA 2015 (see IO.1). The supervisors' understanding of ML/TF risks rests mainly in the identified risks regarding the use of cash and the provision of advice on and the formation of large and complex corporate structures.

403. The RSAA's understanding of risk of the DNFBPs under its remit is also based on their sectoral knowledge of their supervised entities' clients, products and services, and geographic location of conducting business. It is the most advanced in its understanding, identification, and application of these risks. As outlined above for FIs, the RSAA has conducted annual supervisor specific risk assessments since 2015, with the latest version (2018) providing updated views on sector risk mitigation for the most important sectors, assessing residual risk and assigning a risk scoring level for each assessed sector becoming an intermediary for ML. The RSAA has further conceptualised and documented a risk analysis and assessment tool, which resulted in different risk categories, as follows:

Table 6.26. ML/TF Risk Score Rating of DNFBP sectors supervised by RSAA (2018)

ML/TF Risk Score	Type of Obligated Entity
3 – significant risk	Trust & company service providers Real estate & rental accommodation brokers Dealing in goods, for payment in cash of EUR 10,000 or more
2/3 - medium /significant risk	External accounting providers Tax advice service providers
The risk level is defined on a scale of 1-4 (1 = low risk, 2 = medium risk, 3 = significant risk, 4 = very significant risk).	

Source: RSAA

404. Given the exposure of external accounting providers, tax advice service providers, and providers of independent legal services to company formation service business, in addition to the absence of any legal competency admission process for the provision of legal services, the risk assigned is too low, and all three sectors should be considered of significant risk.

405. The NPB/GA and the Bar Association have only commenced and documented their initial and basic supervisor specific risk assessments of the risks of ML and TF of their supervised entities. The NPB/GA has a firmer grasp of the operational ML/TF risks, but the level of sophistication applied needs to increase for both these supervisors to better understand the dynamic ML/TF risks in their sectors.

406. Supervisors need to engage and survey their entities to gain a better sense of the sectors' risks. In this regard, supervisors have yet to progress to conducting desktop or other reviews of sector-based risk assessments compiled by their obliged entities, across all DNFBP sectors. Only the RSAA has made use, albeit limited to some sectors, of their powers to obtain information from obliged entities using risk based surveys or questionnaires.

407. Given the number of entities in each sector, supervisors would be strained to test the validity of the work done by entities, even if a risk-based or sample testing approach is applied. The oversight of obliged entity risk assessments by each DNFBP supervisor may place severe pressure on their capacity and resources. The ability to understand their sector risks is dependent on having adequately skilled staff and processes to evaluate the sector risks. Due to capacity constraints, this is not done adequately or at all by AML/CFT supervisors across all sectors, which in turn diminishes their understanding of the risks in their respective sectors.

Risk-based supervision of compliance with AML/CFT requirements

Financial institutions

408. Overall, the AML/CFT monitoring and supervision of FIs is not carried out on a risk-sensitive basis. Further, both supervisors are significantly under-resourced given the breadth and depth of their AML/CFT responsibilities and associated workload.

409. From 2014 to date, FIN-FSA's ongoing supervisory focus has been predominantly on the banking sector, in particular the three largest banks. For those banks, which are part of cross border groups, FIN-FSA plans its engagement and if necessary coordinates with other Nordic supervisors. There have only been two inspections of the 14 "hawala-type" money remitters despite such firms being considered high risk.

410. FIN-FSA does not carry out any ongoing AML/CFT supervisory engagement (inspections or otherwise) with the majority of the FIs. Rather, the FIN-FSA advises that AML/CFT supervisory engagement for such FIs is focused on the market-entry phase. In practice this means supervisory engagement for most FIs is concentrated and limited to the authorisation process. This approach cannot ensure effective ongoing compliance of supervised firms in the longer term.

411. *FIN-FSA's Ongoing supervision* - Overall, the quantum of ongoing supervision is not adequate. Apart from the three largest FIs that undergo substantial annual engagement, the vast majority of FIs have never been subject to an on-site inspection. Other supervisory tools used by FIN-FSA, such as supervisory visits and targeted questionnaires, are by themselves not sufficient and cannot replace on-site inspections.

412. *FIN-FSA's inspections as part of ongoing supervision* - AML/CFT inspections typically include a review of policies, procedures and associated sampling. Inspections also include examining the implementation of targeted financial sanctions (TFS), although FIN-FSA does not have any statutory powers in this regard (see TC Annex, R. 27). All inspections have included off-site and on-site phases. The on-site aspect of inspections at banks take 3 – 6 days on average, whereas similar inspections at payment service providers and money transfer companies generally last one day. Most inspections take approximately 3-6 months to complete from start to finish. However, on rare occasions inspections (where the scope has been very wide or the inspection has been challenging) can span periods in excess of one year from start to finish (including issuing of post inspection letter).

413. The time and resources allocated to inspections are adjusted according to the size of the FI and the scope of the inspection. The AML/CFT Team, the Prudential Supervisor and, where required, payment system and IT experts have participated in the inspections. AML/CFT-related inspections are executed according to FIN-FSA's guide to the inspection process. The AML/CFT Team has developed AML/CFT inspection procedures and an inspection tool kit used for scoping, data analysis and random sampling.

414. FIN-FSA did not conduct any follow-up inspections in 2014-2017. However, after some inspections, FIN-FSA has conducted follow-up meetings (supervisory visits – see below) and/or requested evidence or documentation regarding corrective measures taken.

415. In addition to planned inspections, FIN-FSA has also carried out four ad hoc AML/CFT inspections of banks with cross border co-operation in 2017, for example following the cases known in English language media as the “Russian laundromat” and the “Panama Papers”. The total number of AML/CFT inspections carried out by FIN-FSA is presented in Table 6.5.

Table 6.27. FIN-FSA AML /CFT Inspections 2014 – 2017

Year	Credit Institutions*	Investment Firms	Payment Service Providers	Other	Total
2017	6	1 (In the same group as a bank)	1	0	8
2016	1	0	1	0	2
2015	1	0	1	1 (finance company)	3
2014	1	0	2	0	3
Total	9	1	5	1	16

Source: FIN-FSA

Note:* A number of banks have been inspected more than once in the period under review

416. *The FIN-FSA's supervisory visits as part of ongoing supervision* - Supervisory visits constitute part of the ongoing supervision framework covering AML/CFT and are part of the annual review-process for the three largest FIs on a quarterly basis⁷⁹. A documented process guide does not exist for supervisory visits and there was little

⁷⁹ FIN-FSA presented the file for one such credit institution evidencing such quarterly supervisory visits as part of the on-site assessment

evidence to suggest that the decisions to undertake such visits were made on a risk-sensitive approach. Supervisory visits are a useful tool in addition to full-fledged on-site and off-site supervision, but being limited in scope and time they cannot substitute inspections and alone are not sufficient to ensure effective compliance of the supervised entities. In 2014-2017 the FIN-FSA carried out 85 supervisory visits.

417. Supervisory visits are generally based on issues that have been identified during ongoing prudential supervision or to follow up on the AML/CFT inspection findings. The figures on supervisory visits are given in the Table 6.6 below.

Table 6.28. FIN-FSA Supervisory visits 2014 – 2017

Year	Meetings with supervised entities
2017	21
2016	21
2015	18
2014	24

Source: FIN-FSA

418. *Other FIN-FSA's Supervisory Engagements* - FIN-FSA has made use of targeted questionnaires to banks on two occasions. The first occasion was in response to a trigger event (see Box 6.3). The second time was in 2017 to pilot the proposed questionnaire being developed as part of its new ML/TF risk assessment process. Questionnaires have not been issued to other sectors to date.

Box 6.25. Case Study: Use of Questionnaires in Supervision

In response to a trigger event, FIN-FSA sent a questionnaire to all financial / banking groups including the biggest branches of foreign credit institutions in Finland. These institutions represent all 230 deposit-taking credit institutions in Finland. In addition, a more detailed questionnaire was sent to a certain bank. FIN-FSA focused mainly on banking groups and branches operating in Finland, since these institutions offer a wide range of banking and investment services and have a large customer base. FIN-FSA requested information of what kind of tax advice the institutions offer or have offered during the past 10 years to their wealth management or other customers. Information was also requested on whether the institutions have offered any services as related to the establishment or administration of offshore structures or whether they have advised or directed customers to contact any other legal service provider for that purpose. To verify the responses FIN-FSA has held a number of meetings with certain FIs.

FIN-FSA decided to conduct an on-site inspection in one FI. Only a very small number of Finnish citizens as customers were detected and the services the inspected FI was providing did not appear to include advice for establishment or administration of offshore constructions. FIN-FSA's inspection did not reveal any significant findings in this matter so no further supervisory actions were needed.

419. *FIN-FSA Resources* - AML/CFT supervision is managed by FIN-FSA's Operational Risks Division. The division currently employs four permanent AML/CFT experts and one on a fixed-term contract until the end of 2018. The number of AML/CFT experts averaged approximately 2-3 persons at any given time during the review period. The team is led by the Head of the Operational Risks Division and reports directly to the Head of Department who reports to the FIN-FSA management group on AML matters.

420. The AML/CFT team's duties include the supervision and inspection of AML/CFT strategies employed by financial market entities, organising of AML/CFT activities, and the evaluation of operating models and practices upon market entry (i.e. permits, registrations and notifications) as well as ongoing supervision of FIs under its remit. The team is also tasked with the preparation of official FIN-FSA guidelines, regulations and opinions addressed to its supervised entities. In addition, the team cooperates with other domestic and international supervisory authorities and stakeholders, participates in domestic and European regulatory policymaking, trains and educates its supervised entities, and replies to customer queries.

421. The AML/CFT Team consists of a good mix of technical and legal expertise, and the team clearly demonstrates strong motivation and commitment to the work it undertakes. However, the team is significantly under-resourced given the breadth and depth of its AML/CFT responsibilities and associated workload. The departure of a single team member may put at risk the functionality of the whole team.

422. *The RSAA's supervisory activities* - There was little evidence that the risk assessment prepared by the RSAA (see Table 6.3) was used in any systematic or meaningful way as a basis in its supervisory planning. Rather, the annual supervisory plan is drawn up by the team on the basis of (i) engaging with sectors where there has been little engagement thus far⁸⁰, (ii) increasing its knowledge of such sectors, (iii) seeking confirmation that information on the currency exchange and company service provider registers is correct and (iv) following up on previous supervisory campaigns. RSAA also has responsibility for AML/CFT supervision of other FIs such as financial leasing, advice on corporate acquisitions and restructuring etc. as such firms do not require authorisation to operate. The RSAA estimates that the population of such FIs is approx. 2 500⁸¹. Further, the RSAA has only commenced formal on-site/off site inspections in 2017 with five on-site and two off-site inspections of currency exchange businesses. Notwithstanding this, with regard to the FIs under its remit, the RSAA has concentrated its supervisory efforts over the four years to 2017, on currency exchange businesses⁸² which it has rated as being of "Significant Risk" (see Table 6.3).

423. *Other RSAA Measures* - The RSAA also makes use of questionnaires as part of its supervisory engagement. For example questionnaires were issued to consumer credit providers in 2012 and 2017 and to currency exchange businesses in 2015.

⁸⁰ Predominantly on the DNFPB side

⁸¹ While the RSAA has made efforts to identify such firms through the trade registers etc., it is impossible to ascertain the definitive population in absence of a registration requirement. Amendments the AML/CFT Act will require such FIs to register with the RSAA with effect from 1 July 2019.

⁸² The RSAA is also supervisor for a number of DNFPBs and much of its supervisory engagement is centred on such entities. See section below for the RSAA DNFPB engagement in this regard.

Such questionnaires seek information on activities and on the FIs AML/CFT compliance frameworks, and are used to further the RSAA's understanding of the FIs it supervises.

424. *RSAA Resources* - The RSAA is under-resourced given the breadth and depth of its AML/CFT responsibilities and associated workload. The relevant RSAA team currently comprises four persons. This team is responsible for registration, ongoing supervision, all policy/guidance and outreach to both the FIs and DNFBPs under the RSAA's remit. The team is very proactive in its approach to furthering its knowledge and assessment of the risks in the FIs it supervises but for those sectors with which it has not had significant engagement, knowledge is more limited.

DNFBPs

425. Overall, the varying levels of supervision of the DNFBP sectors do not meet the required standard of AML/CFT supervision and this has a significant impact on the effectiveness of the AML/CFT supervisory regime. Supervisors have not been effective in mitigating the risks, as they have not gathered the necessary knowledge to commence risk sensitive supervision and do not have the capacity and processes in place to systematically monitor the state of compliance of obliged entities. The current capacity of supervisors compared to the potential universe of sector participants they have to supervise is significantly inadequate.

426. Moreover, the regional gaming operator, while licensed under the Åland Regional Lotteries Act, is not currently subject to any AML/CFT supervision under the 2017 AML/CFT Act, but is supervised for general gaming operations by the Ålands gaming supervisor, the Åland Lotteriinspektion.

427. Only a few supervisors have actually commenced on-site AML/CFT inspections, e.g. the 2017 RSAA inspections of 10 real estate agents, and 4 NPB/GA inspections which were directed and limited to the mainland casino and have identified compliance shortcomings which have required remedial actions by the inspected entities. The NPB/GA only obtained inspection powers under the 2017 AML/CFT Act.

428. As DNFBP supervisors received AML/CFT inspection and sanctioning powers in July 2017, inspection planning was in the development phase at the time of the on-site visit and the methodology to apply risk-based supervision of compliance with AML/CFT requirements was also under consideration. The RSAA has commenced compiling an AML/CFT inspection manual which is not yet final. Generally, DNFBP supervisors are in the early stages of considering and documenting what would constitute their risk-based supervision approach to compliance with AML/CFT requirements. Although most supervisors embrace a risk-based approach to supervision, they have yet to exercise their supervisory activities in a risk-based manner.

429. There has been no RSAA supervision (including inspections) of independent providers of legal services, accountants, and tax consultants, but limited supervision of dealers in precious metals and stones, under the 2017 AML/CFT Act. The RSAA has not yet conducted a supervisory campaign for the legal services providers sector, and has no documented view on how obliged entities in that sector understand their ML/TF risks, and what mitigation measures are to be applied.

430. The Finnish Bar Association has added the AML/CFT inspection process to the annual auditing of the general work of selected practicing attorneys. They plan to execute only 80 dedicated AML/CFT inspections in the coming year.

431. As mentioned above, the relevant RSAA team currently comprises four persons and is under-resourced given the breadth and depth of its AML/CFT responsibilities and associated workload. The Bar Association is building capacity to conduct AML/CFT supervision. An inspecting lawyer has recently been hired by the Bar to coordinate supervision and conduct the offsite work. The on-site inspections will be carried out either by inspecting lawyers designated by the local branch –peer supervision approach- or by the inspecting lawyer of the Bar Association, or in co-operation between the two. The Bar Association has trained 50 attorneys from local branches to ensure that each attorney's office can be inspected every six years. The NPB/GA increased its resources in 2017, from approximately 1/3 of a man-year to slightly less than one man-year, and it is planned to recruit two new people to support the AML/CFT supervision work. The NPB/GA should consider recruiting more supervision staff, particularly if the Government plans to open a second casino in mainland Finland in the very near future. The turnover of people in charge of gaming supervision at the NPB/GA could impact the continuity of the work and the full understanding of the exposure of gaming activities to ML/TF.

Remedial actions and effective, proportionate, and dissuasive sanctions

Financial institutions

432. As of June 2018, notwithstanding the availability of a range of supervisory and enforcement measures, neither FIN-FSA nor the RSAA have imposed any administrative sanctions with regard to ongoing compliance with AML/CFT obligations on the FIs they supervise. As such, it cannot be said that effective, proportionate and dissuasive sanctions have been issued. Both authorities place emphasis on remediation of AML/CFT deficiencies discovered during inspections and other engagement.

433. Both FIN-FSA and the RSAA advise that administrative sanctions are considered if the issues identified during inspection and other engagements are not corrected in an appropriate manner or within the timetable required. However, given the limited number of inspections and other engagements as mentioned earlier, this approach is not adequate.

434. There is also a danger that the effectiveness of this supervisory approach could be undermined in the absence of a credible and enforced sanctions regime to follow through with FIs on identified weaknesses. It is widely observed that the “credible threat” and imposition of sanctions is an effective measure in achieving compliance both at a firm level and across sectors by allowing peers to undertake a gap analysis where such sanctions are published.

DNFBPs

435. DNFBP supervisors across the board have not yet applied any administrative sanctions for AML/CFT non-compliance since obtaining sanctioning powers, in July 2017. Accordingly, while detailed administrative sanctioning powers are available to supervisors under the AML/CFT Act, it cannot be said that any effective,

proportionate and dissuasive sanctions have been issued. However, this is understandable given the scope of compliance obligations under the 2017 Act, which the DNFBP supervisors are arguably seeking to bed down through improving compliance understanding amongst obliged entities in the first year of application of the 2017 Act.

436. Supervisors lack powers to supervise the implementation of targeted financial sanctions (TFS) for TF, although they do check that the necessary processes are in place when conducting the licence granting process. Therefore there have been no sanctions imposed in this field.

Impact of supervisory actions on compliance

Financial institutions

437. Overall, the supervisors have not been able to demonstrate that their actions have an effect on compliance by financial institutions.

438. FIN-FSA's emphasis on the quality of risk assessments at time of authorisation has increased awareness amongst FIs of the importance of bespoke assessments as opposed to generic assessments.

439. The lack of follow-up inspections and the limited nature of other engagement by FIN-FSA with the majority of FIs makes it difficult to gauge the impact and effectiveness of its supervisory actions on FIs' compliance with their AML/CFT obligations. There has been an increase in both AML/CFT personnel resources (1st and 2nd line of defence) and technical AML/CFT tools (such as transaction monitoring) within Finnish FIs particularly in the larger banks. However, contrary views exist between the private sector and FIN-FSA as to whether this is a result of supervisory action.

440. The RSAA has not conducted any follow-up inspections or follow-up engagement to ensure that requested remedial actions have been put in place or that their supervisory actions have been effective. Again this makes it difficult to gauge the impact and effectiveness of its supervisory actions on FIs' compliance with their AML/CFT obligations.

DNFBPs

441. It is difficult to gauge the impact of supervisory actions on compliance across DNFBP sectors, as few and intermittent supervisory engagements with obliged entities have been held. The low number of inspections conducted and only in certain sectors, means that virtually no impact of supervisory action can be demonstrated at this stage.

Promoting a clear understanding of AML/CFT obligations and ML/TF risks

Financial institutions

442. FIN-FSA seeks to promote the understanding of ML/TF risks and AML/CFT obligations through its authorisation and ongoing supervisory engagement. It also provides some guidance to FIs through different channels (e.g. website, newsletters, etc.). Such outreach includes meetings and training sessions with various industry representatives and stakeholder groups, issuing AML guidance and binding

requirements, and periodically publishing a newsletter on AML topics on its website.

443. The RSAA has undertaken outreach to improve AML/CFT awareness by supervised entities. Such outreach includes the publication of general and sector specific AML/CFT guides, providing training at industry events on AML/CFT related topics and conducting supervisory campaigns comprising the issuing of questionnaires to consumer credit providers and currency exchange providers which served the dual purpose of gathering more information for the RSAA and also raising the overall awareness of AML/CFT obligations by the firms who completed the questionnaires.

444. While the above efforts of both FIN-FSA and the RSAA are acknowledged, there are known weaknesses in certain FIs' risk identification and AML/CFT compliance (for example certain sectors, smaller entities or new market entrants) that have not been proactively targeted or addressed. Furthermore, all FIs have expressed the need for further guidance particularly with regard to application of AML/CFT legislation and with regard to the identification of TF issues and typologies.

DNFBPs

445. DNFBP supervisors such as the RSAA, the NPB/GA, and the Bar Association (also assisted by Real Estate Associations) have commenced outreach to improve an understanding of ML/TF risks and AML/CFT obligations among their supervised entities. In particular, the RSAA undertook a supervisory campaign in 2015 with dealers in precious metals and stones on awareness of AML/CFT obligations and regarding the risk of cash dealing, and a supervisory campaign in 2016 with the real estate sector and trust and company service providers regarding their AML/CFT obligations and risks of cash in their activities. The RSAA has not engaged at all the providers of independent legal services and tax advisors to promote a clear understanding of the AML/CFT obligations and ML/TF risks.

446. To improve understanding, in addition to the publication of two AML/CFT general guides (see above), RSAA engages with most sectors on ML/TF risks and AML/CFT obligations. The Bar Association's first guide for complying with AML/CFT requirements was published in 2009 and the second in September 2017. The Real Estate Associations have also prepared awareness material on the AML/CFT requirements for their members. Nevertheless, they have both expressed the need for more detailed guidance from the RSAA, particularly in regard to SDD and EDD measures. However, there is little co-ordination between the Finnish Bar Association and the RSAA (who is empowered to ultimately sanction non-compliant attorneys). Both supervisors would benefit by engaging more regularly.

Overall conclusion on IO.3

447. **Finland has achieved a low level of effectiveness for IO.3.**

CHAPTER 7. LEGAL PERSONS AND ARRANGEMENTS

Key Findings and Recommended Actions

Key Findings

- a) There is a variety of legal persons that can be created in Finland. Processes for the creation of those legal persons, as well as for obtaining and recording basic ownership information are described in the legislation, as well as on the public websites, which are accessible online without restriction.
- b) While it is not possible to establish trusts under Finnish law, a foreign express trust may nevertheless have a presence in Finland, do business in Finland (e.g. buying assets or contracting), and be a client of obliged entities, in particular banks.
- c) Vulnerabilities involving legal persons and the potential for company misuse by criminals are generally understood. Law enforcement, supervisory authorities and obliged entities acknowledge that corporates and complex corporate structures (especially with foreign ownership) remain attractive to criminals operating in Finland and could be misused for ML.
- d) Finland has in place certain preventive measures, however they are not effective with regard to the most risky types of legal persons, often misused for tax evasion purposes.
- e) The public registries of legal persons are not fully reliable, as data is verified for accuracy and relevance only when it relies on the Finnish Population Information System and Legal Register Centre. Resources devoted to verification of paper-based notifications are inadequate.
- f) Since there is no meaningful supervision of the company service providers (see IO. 3), it leaves them open to misuse when they engage in company registration or serve as nominee directors for the companies.
- g) The ability of competent authorities to establish the beneficial ownership (BO) of legal persons in a timely manner is very limited. In most risky scenarios, i.e. when there is foreign ownership involved, the time needed to establish BO is significant and can take up to several months.
- h) The remedies to ensure that registered information is kept up to date are not fully appropriate, as both the failure to keep registered information up to date as well as deliberately submitting false information into the register are sanctioned as penal/criminal offence. The Finnish Patent and Registration Office (PRH) does not have a legal right to make use of any administrative sanctions other than proceeding with deregistration in certain circumstances.

Recommended Actions

Finland should:

- a) In light of the grey economy and ML/TF concerns, undertake a fully dedicated risk assessment on the misuse of all the legal persons, foreign express trusts and similar legal arrangements, as well as non-profit associations, in Finland.
- b) Require trustees of foreign trusts to disclose the fact of operation to competent authorities, which practically speaking may take the form of disclosure through a publically accessible register of foreign trusts doing business in Finland.
- c) Promote effective supervision and enforcement of BO transparency obligations, through a multi-agency approach, involving the Tax Administration, the National Bureau of Investigation (NBI) and the FIU, other law enforcement agencies and the designated supervisory authorities,
- d) Implement the most appropriate measures to mitigate the misuse of legal persons and legal arrangements (such as de-registering fraudulent or dormant companies), and the activities of their front men and agents.
- e) Put in place adequate verification personnel and more robust measures to ensure the accuracy of information in all publically held registries, at all times, as a necessary precursor to the establishment of a national BO register.
- f) Empower PRH to issue administrative sanctions for failure to submit adequate, accurate and up-to-date information, where appropriate.

448. The relevant Immediate Outcome considered and assessed in this chapter is IO.5. The Recommendations relevant for the assessment of effectiveness under this section are R.24-25.⁸³

Immediate Outcome 5 (Legal Persons and Arrangements)*Public availability of information on the creation and types of legal persons and arrangements*

449. Different types of legal persons under private law are identified and described in the relevant legal acts (see R.24 for more details). The processes for the creation of those legal persons, as well as for obtaining and recording basic ownership information are described in the legislation, as well as on the public websites of the Business Information System (BIS)⁸⁴ and Finnish Patent and Registration Office (PRH)⁸⁵.

⁸³ The availability of accurate and up-to-date basic and beneficial ownership information is also assessed by the OECD Global Forum on Transparency and Exchange of Information for Tax Purposes. In some cases, the findings may differ due to differences in the FATF and Global Forum's respective methodologies, objectives and scope of the standards.

⁸⁴ www.ytj.fi

⁸⁵ www.prh.fi

450. Finland is a highly digitised economy and has in place extensive publically accessible registries containing basic ownership information on legal persons. BIS is an online portal administered by the PRH and the Tax Administration. It consists of two PRH registries: the Trade Registry of companies and businesses, and the Register of foundations, plus the VAT, Prepayment and Employer Register administered by the Tax Administration. The Register of Associations, and Register on Religious Communities exist separately and are accessible on the PRH website.

451. Express trusts or other comparable legal arrangements cannot be established under the Finnish law.

Identification, assessment and understanding of ML/TF risks and vulnerabilities of legal entities

452. No comprehensive or dedicated vulnerabilities assessment has been undertaken with regard to legal persons. However, it appears that in Finland the relevant competent authorities have a reasonable understanding of the ML/TF risks posed by legal persons. Legal persons, particularly with foreign ownership, with some using front men, were identified as presenting high risks for ML in the NRA 2015. The use of complex corporate structures and “front men” in tax and ML schemes were frequently cited by tax authorities, law enforcement and the FIU. The work done on the grey economy (see Chapter 1 and IO.1) also informs this level of understanding. The authorities acknowledge that overall legal persons, foreign trusts and similar legal arrangements, remain very attractive for misuse by criminals for ML and TF.

Mitigating measures to prevent the misuse of legal persons and arrangements

453. Finland has in place certain preventive measures; however, as explained below, they are not effective with regard to the most risky types of legal persons, particularly those misused for tax evasion purposes.

Company registers

454. Finland has in place publicly accessible registries containing basic ownership information on legal persons, through the BIS system and other relevant registries, however the accuracy of that information is not ensured in all cases. The basic information kept in the BIS reflects the latest information, date of capture, and information source (PRH or Tax Administration or common), status of registrations in force, and Legal Entity Identifier (LEI) status, relating to the following elements:

- Trade name – (PRH);
- Parallel trade name – (PRH);
- Company form – (PRH);
- Home Municipality – (PRH);
- Language – (Tax Administration);
- Main line of business – (Tax Administration);
- Postal Address – (common);
- Street Address – (common);
- E-mail – (common);
- Registrations in force – (e.g., Foundations Register, Tax Administration);

- Status of Registration and Date – (Registered as of [date]);
- Tax Debt Register – (link provided to access);
- Business ID History – (Date and Event – ID Given);
- LEI Details - (LEI Code number; LEI Status; Start Date and Register e.g. Finnish BIS);
- Show LEI Code History – (detail provided).

455. The Trade Register specifically can provide additional information about the Business ID of the company, and the details and roles of persons involved in the company, inter alia, as follows:

- Business ID – (Number);
- Entered in the register – (Date);
- Home page address – (website details);
- Persons details – (Role of Legal person; Name, domicile and country; identity code and register; legal form)
- Role of natural person – (Director, authorised, foreign representative);
- Surname, first names / company name
- Date of Birth / Identity Code;
- Citizenship; and
- Name History and date.

456. Natural persons are required to notify the PRH and Tax Administration through online application or paper-based filing notices when they establish a legal person or start up a business, make changes to them or terminate them. They are further required to submit company address information to both the Finnish Post Office (*Posti*) and to the BIS when they start up a business or company, set up a new office, or change the name of the company. They must also inform *Posti* if their home address is the postal address of their company.

457. Electronic application is available to those persons who possess electronic Finnish ID which is issued by the Finnish government on the basis of the Finnish Population Information System, which sits at the heart of personal identification, and is the most used basic register in Finland. It is a computerised national register, accessible online, that contains basic information about Finnish citizens and foreign citizens residing permanently in Finland. It therefore acts as an information base of detailed particulars of natural persons involved in business and legal person activity. The personal data recorded in the system includes name, personal identity code, address (unless barred), citizenship, native language, family relations, and date of birth and death (if applicable). The information held in the Finnish Population Information System is reliable as it is verified by the Finnish authorities maintaining it. The information on the Finnish natural persons involved in legal persons, their shareholders and managers, which are created via electronic application process is therefore accurate and easily accessible.

458. However, as mentioned above, such electronic registration is only available to Finnish residents and moreover it is not mandatory. If a legal person has at least one shareholder or manager who is not a Finnish resident, then the registration has to be done through paper-based application, which is mainly the case with the formation of foreign-owned company branches or subsidiaries in Finland. Finnish residents may also opt for a paper-based registration of legal persons. This can be

done in person at the offices of the PRH or by submitting all necessary documents by post. In regard to whether the public registries of legal persons contain accurate data relating to basic information, the quality of accurateness is largely determined by the ability of the authorities to verify the information relating to basic information in each registry, at any time.

459. The PRH has in place procedures and controls on the management of the registry information, but they are limited to checking whether all necessary documents have been submitted and legal prerequisites for corporate registration have been met. The PRH does not adequately verify, nor is it resourced to do so, the authenticity of the documents at any stage before incorporating such information in the trade registry. This is especially the case where the submitted information is paper-based. There are not sufficient mechanisms in place to ensure the information previously submitted remains up-to-date. The PRH approach to the basic information kept in the trade registry applies similarly to the Foundations and Associations registries under their administration.

460. There have been cases of fraudulent paper-based applications for foreign applicants as well as the hi-jacking of existing registered corporates (mostly dormant) by criminals who manipulate the company information and use the compromised legal persons to conduct unlawful activities. This points to deficiencies in the ability to keep basic information in the BIS registries accurate and secure, and not able to be abused by criminals. This has a cascading effect, as many other public registries, obliged entities and private sector in general place reliance on the correctness of the trade registry in Finland. Only recently, the handling process of the PRH regarding electronic and paper-based notifications (relating to both notifications of establishment and amendment) has included measures aimed to ensure reliability in respect of the registered information (such as contacting the current owners before making changes to the registry).

461. There are no mitigating measures in place regarding the abuse by criminals of foreign formed legal arrangements operating in Finland. Finnish law enforcement and tax authorities have indicated that certain complex matters, often having an extra-territorial dimension or involving foreigners, do involve the use of complex corporate structures, including, in individual cases, foreign express trusts, and similar legal arrangements. This remains a vulnerability, but should be addressed by requiring BO information on foreign express trust operating in Finland to be kept as part of the revised BIS public registry system in 2019.

Bearer shares

462. Finland has prohibited the issuance of bearer shares since 1 January 1980, and considers that only a marginal number of such shares still exists. The 2013 peer review by the OECD's Global Forum on Transparency and Exchange of Information for Tax Purposes⁸⁶ contains the estimate of approximately 9 400 companies that had been incorporated before 1 January 1980 which were still in existence and active at that time. That represented less than 5% of the total number of all companies. These 9 400 companies could have potentially issued bearer shares if their articles of association allowed them to do so. There were no specific statistics on how many of

⁸⁶ See www.oecd-ilibrary.org/taxation/global-forum-on-transparency-and-exchange-of-information-for-tax-purposes-peer-reviews-finland-2013_9789264191938-en

the 9 400 companies could issue bearer shares pursuant to their articles of association, if any of them had issued bearer shares and if any bearer shares were still in circulation. However, none of the entities or authorities interviewed had encountered them in practice. This leads the assessment team to believe that the risk of the misuse of existing bearer shares is low. There appears to be appropriate mechanisms in place to identify the holder of bearer shares still in circulation in Finland. In particular, various reporting obligations which apply to both companies and shareholders (including the holders of bearer shares) ensure that any holder of an existing bearer share certificate is identified, before they would be permitted to exercise any rights attached to such bearer share.

Nominees

7

463. Nominee shareholders and nominee directorships remain areas of vulnerability in the corporate landscape in Finland. There is no explicit prohibition on nominee shareholders or directors in Finland, and the concept of nominee ownership exists in Finland in relation to shares in book-entry form. Most limited liability companies in Finland issue shares in certificate form, and such shares are deemed by the Finnish law to be owned by the person whose name is recorded in the share register maintained by the company. Therefore, all the benefits and consequences of owning the shares will apply to the person reflected as the owner of the shares in the share register. This limits, but does not exclude, the potential for misuse by professional nominees.

464. While Finland has not observed any active professional market for company incorporation and management, there are approximately 58 company service providers (who tend to be mainly attorneys, accountants, or independent legal services providers) (see Table 1.2 in Chapter 1). Since there has been no on-site supervision of these company service providers based on the AML/CFT Act in force since July 2017 up until the time of the FATF on-site visit (see IO.3), it leaves them open to misuse when they engage in company registration or serve as nominee directors for the companies.

Timely access to adequate, accurate and current basic and beneficial ownership information on legal persons

465. Timely access to adequate, accurate and current basic and beneficial information is only possible for legal persons that were established using the electronic application process through the BIS registries, which essentially means that the ownership chain up to the natural person remains in Finland. This information is public and can be accessed online in a timely manner.

466. Information on other types of legal persons, which have been established using paper-based notifications, is not of same degree of reliability and is of limited use. This was confirmed during the discussion with law enforcement and other competent authorities who expressed concern regarding the accuracy of basic information in the business information system, including trade registry.

467. The availability of BO information does not rely only on the existence of registries, as law enforcement can source some BO information from obliged entities who have applied appropriate CDD or EDD measures in this regard, as well as through the shareholder register at the head office of the company, which is accessible to everyone. This avenue is not sufficient and is not timely as it requires knowledge of where to look, which obliged entity to approach for the information, and is further dependent on the level of record keeping, which is adequate among financial institutions, but may not be sufficient among DNFBPs (see IO.4). Moreover, if there is a foreign ownership of a Finnish company, it may take competent authorities substantial time, up to several months, in order to establish the beneficial owner, e.g. if there is a need to request international assistance (see IO.2).

468. Overall, timely access to adequate BO information on all types of legal persons created in Finland is not currently possible. Finnish authorities intend to create a national BO registry by extending the current BIS to include the Register of Associations and Register on religious communities, and to further extend the Trade Registry to include full BO information on companies and businesses, by 1 July 2019.

Timely access to adequate, accurate and current basic and beneficial ownership information on legal arrangements

469. The Finnish legal system does not allow for the creation of trusts.⁸⁷ While the legal concept of trust does not exist under Finnish law, the 2017 AML/CFT Act introduces provisions that define a “foreign trust” and that describe the “beneficial owner of a foreign trust” or trust like arrangement. This acknowledges that trustees of foreign express trusts may operate in Finland. Foreign trusts doing business in Finland would be clients of obliged entities, and may be a client of a Finnish bank if it requires banking facilities in Finland. Further, a Finnish resident may act as a trustee of a foreign trust. The foreign trust, as customer to an obliged entity, would be subject to the CDD, including BO, record keeping and reporting requirements, although in practice the competent authorities and financial institutions have rarely observed trustees of foreign trusts operating in Finland.

⁸⁷ Finland has not ratified the 1985 The Hague Convention on the Law Applicable to Trusts and on their Recognition.

470. Finnish authorities intend to create a BO registry with registration starting by 1 July 2019. It is contemplated that such registry would make provision for the record of BO information relating to foreign express trusts operating in Finland.

Effectiveness, proportionality and dissuasiveness of sanctions

471. Finnish authorities have not applied any sanctions against persons who have not complied with the information requirements. The remedies to ensure that registered information is kept up to date are not fully appropriate, as both the failure to keep registered information up to date as well deliberately submitting false information into register are sanctioned as penal/criminal offence. PRH does not have a legal right to make use of any administrative sanctions other than proceeding with deregistration in certain circumstances.

7

Overall conclusion on IO.5

472. **Finland has achieved a moderate level of effectiveness for IO.5.**

CHAPTER 8. INTERNATIONAL CO-OPERATION

Key Findings and Recommended Actions

Key Findings

- a) Finnish authorities provide timely and useful mutual legal assistance (MLA) to foreign authorities. Finland also execute European Arrest Warrants efficiently and speedily. There was no ML/TF-related extradition request over the last years.
- b) Finnish authorities request MLA to the extent needed to build cases. MLA requests are generally in line with Finland's geographic risk exposure.
- c) All relevant authorities in Finland – including the FIU, the National Bureau of Investigation (NBI) and police forces in general, Customs and tax authorities – routinely seek and provide international cooperation for AML/CFT purposes, as part of their normal course of operations. Target countries reflect the main national geographical risks. Information is provided mainly on request, but also spontaneously. Exchanges of information are formal and informal. They support analytical and operational work, including ML/TF investigations.
- d) There is good international co-operation for the supervision of international financial institutions (FIs)/groups. International co-operation of supervisors of other obliged entities is limited, in line with the domestic scope of activities of these businesses and professions.
- e) Competent authorities are able to provide basic information on legal persons registered in Finland. Finnish authorities provide information to their international counterparts on beneficial ownership (BO), but the timeframe to access and check the information can be long.

Recommended Actions

Finland should:

- a) Keep statistics on MLAs related to ML and TF, including to/from Nordic and EU countries, in order to improve its understanding of ML/TF risks.
- b) Equally, keep track of exchanges of basic and BO information on legal entities and arrangements.

473. The relevant Immediate Outcome considered and assessed in this chapter is IO.2. The Recommendations relevant for the assessment of effectiveness under this section are R.36-40.

Immediate Outcome 2 (International Co-operation)*Providing constructive and timely mutual legal assistance (MLA) and extradition*

474. Finnish authorities provide timely and useful MLA to foreign authorities. Based on the feedback from FATF global network members on the provision of MLA by Finnish authorities on ML/TF related cases, there is a good level of co-operation and satisfactory responses from Finnish authorities, and co-operation is timely. Finland routinely provides bank and other business records, as well as assistance in identifying, seizing and forfeiting the proceeds of crime.

475. Finland estimates that the handling of incoming MLA requests, mainly for cases related to fraud or embezzlement, usually takes around 1-2 months. For urgent cases, for example if the person is under detention or if funds can be frozen, the request is handled immediately. The National Bureau of Investigation (NBI), part of the Police, is one of the main receivers of MLA requests. A majority relate to information concerning Finnish virtual currency operators (see ex. in Box 8.1). Another major target is "package mules" that have operated in the eastern part of Finland and have been subject of cooperation primarily with German law enforcement and judicial authorities.

Box 8.26. Provision of MLA by Finnish authorities in a virtual currency case

Law enforcement authorities of an EU Member State were investigating aggravated ML. Finland received a request for information regarding the users' names of a domestic virtual currency operator's customers. These user names had been used to convert Bitcoin to Euro. This service had been provided at a higher cost than usual, and the process had been anonymous.

The foreign LEA suspected two persons of ML and of participation in the activities of an organised crime group. The MLA request was made to clarify information about the users of the accounts, as well as possible message flows between the account users.

The requested information was obtained from the Finnish virtual currency operator and delivered to the requesting foreign LEA.

476. Finland's use of MLA is generally in line with the country's risk exposure. The Ministry of Justice indicated that MLA is mainly provided to Russia, Turkey and the United States, and within Europe to Sweden and the Nordic countries as well as to Germany, Estonia and Poland for fraud-related crimes, and Spain and the Netherlands for drug-related crimes.

477. Regarding extradition, Finland receives on average less than 15 requests per year from non-EU and non-Nordic countries. However, in all extradition cases reviewed up until 2003, there were none based on ML/TF.

478. Finland executes European arrest warrants (EAWs) efficiently (few refusals) and speedily (matters of days or weeks). In 2017/18, there were six ML related EAW

cases of which two from Nordic Countries. In two of them, aggravated ML was the main offence; in three others, the ML offence was connected to fraud and other property crime; and in one to an aggravated narcotics offence (see examples in Box 8.2.).

Box 8.27. Examples of EAWs executed by Finland for ML offences

Example 1 involved laundering proceeds of a hacking offence to accounts of a Danish bank. Fraudulent funds arrived to accounts held by individuals residing in Belgium and were transferred to Russia. The person surrendered (Russian) to Belgium, convicted and sentenced to three years, acted as part of a criminal organization, at least recruiting other persons involved.

Example 2 involved laundering proceeds of hacking the information system of a British bank. GBP 60 000 were transferred to the surrendered person (Estonian) to Estonia, convicted and sentenced for two years, in two bank transfers and the person transferred it in cash forward.

Example 3 involved laundering proceeds of an unspecified crime (presumably fraud). EUR 6 000 were transferred from the victim's German bank account to the surrendered person's (Latvian) bank account in Czech Republic. The money was directly transferred to a Latvian bank account and directly withdrawn from there.

479. The lack of comprehensive and detailed MLA statistics could impact Finland's understanding of ML/TF risks. Due to the direct contact between the relevant Finnish authorities and their counterparts from Nordic countries and EU Member States, some information concerning MLA co-operation is not reflected in consolidated statistics. There are global figures available for MLA with non-Nordic countries and non-EU Member States (see Tables 8.1 and 8.2), with only estimations, based on known cases, of ML/TF-related cases. Nevertheless, the Police maintains statistics on incoming and outgoing requests, from which requests related to ML and TF offences may be extracted. Maintaining detailed and comprehensive MLA statistics, also to/from European countries, including the countries with which there are MLA flows and the requesting authorities, would help Finland map transnational ML, TF and predicate offences, and get a better understanding of its ML/TF risks.

Table 8.29. Requests for MLA - non-EU Member States or non-Nordic countries, for all crimes (known ML cases in brackets)

	2014	2015	2016	2017
Sent	58 (8)	68 (8)	84 (13)	50 (3)
Received	97 (2)	99 (-)	71 (3)	86 (2)
Total	155 (10)	167 (8)	155 (16)	136 (5)

Source: Finnish authorities

Seeking timely legal assistance to pursue domestic ML, associated predicates and TF cases with transnational elements

480. MLA is sought by Finnish authorities to the extent needed to build their cases. As outlined in the beginning of this chapter there is no comprehensive data available on outgoing MLA requests to Nordic or EU authorities, and no specific ML/TF-related quantitative data. However, and based on discussions held with relevant authorities and cases referred to by them, MLA is used whenever necessary. In general, once a decision to conduct an investigation is made, Finland sends MLA requests to every country that is involved. Requests are sent to both EU and non-EU countries that could potentially have relevant information on the same case, even though some countries would rarely provide any response. Finnish authorities mentioned a TF case in which an MLA request was sent to a country where the brother of the suspect had been in prison, which provided a useful lead for the investigation (see Boxes 4.1 and 4.5 in IO.9).

Box 8.28. Examples of MLA requests from Finnish authorities

Highway case - The FIU was informed by a commercial bank about suspicious money transfers from Russia to Finland. Over EUR 9 million worth of funds of a Finnish company were frozen. The NBI launched a criminal investigation on suspicion of aggravated ML. It established that a total of EUR 100-150 million was transferred to Finland and that the funds were transferred from Russia for the (fake) construction of a motorway and border crossing point in Karelia, on the Russian side of the border. A number of MLA requests were made around the world in order to trace the funds, including in Russia, Latvia and Cyprus, which were countries to which funds had been transferred. The case is still ongoing.

Cargo case - A group of Russian couriers carried over EUR 20 million from an Estonian bank to Russia via Finland during an approx. eight-month period in 2011-2012. The funds were sent to the Estonian bank from Russia and returned to the sender in cash. It has also been confirmed that assets were circulated through a complicated arrangement, using companies established in New Zealand and the USA, and a number of fake contracts and invoicing documents. An FIU case was opened and EUR 3, 6 million worth of funds frozen. A criminal investigation was opened and MLA requests were sent to a number of foreign countries with which the case had connections (Denmark, Estonia, Latvia, New Zealand, Russia, UK and the US). In 2015-16, a criminal investigation was opened in Russia. The case is still ongoing.

481. Finland faces challenges repatriating assets, although requests are made to the relevant foreign authorities (see IO.8). A significant portion of the proceeds of crimes generated in Finland are moved outside of the country and may not be seized at the criminal investigation stage. In those cases, enforcement of confiscation relies heavily on international co-operation. Although a comprehensive overview could

not be provided (see below), Finland presented some cases in which it filed formal requests to foreign countries, including through the EU Confiscation mechanisms, to seek the repatriation of assets (see Table 3.18 and Box 3.12 in IO.8). As mentioned in 8.2.1 above, there is a need to refine the quantitative data available on European MLA, including on confiscation (see IO.8), to support the identification and assessment of ML/TF risks in the country.

Seeking and providing other forms of international co-operation for AML/CFT purposes

482. *FIU* - The FIU frequently seeks international co-operation from its counterparts and other authorities to support its analytical and operational work. The FIU sends outgoing requests to countries with connections to STRs received, regarding the nationality of people involved, the place where businesses involved are registered, the origin/destination of the financial transaction(s), etc. FATF delegations which provided feedback on their interaction with the Finnish FIU mentioned receiving requests in cases related to serious fraud, tax fraud, aggravated ML, and CFT related cases. The FIU uses the information received from abroad to support and enrich its operational and tactical analysis and build connections with ongoing ML/TF cases, or initiate ML/TF cases.

Box 8.29. Example of FIU co-operation with foreign counterparts

*Dominica case*⁸⁸ - The FIU opened a case to analyse an incident in which a payment card had been used to withdraw assets to the value of over EUR 230 000. The Finnish FIU sent a first request for information to the Finnish bank having issued the card. Additional requests were sent, among others, to other Finnish banks, and the FIUs of Latvia, the Dominican Republic, Brazil and Poland.

The Finnish determined that the Brazilian husband of the owner of the bank account to which the payment card was linked had established a company in the Dominican Republic and opened a bank account for the company in a Latvian bank. Following this, the husband sold consultancy services to a very large Finnish company, charging the company nearly EUR 740 000, whilst claiming not to be liable to taxation in Finland. Eventually it was found out that the husband had not paid taxes to any country and was a Finnish taxpayer based on his residence.

The FIU disseminated the case to the Tax Administration which reported the case to the police. A criminal investigation for aggravated ML was started. The subject is suspected of having avoided paying income tax to the value of EUR 342 259.48. The case is pending.

483. The countries from which the FIU mainly seeks information are consistent with Finland's overall geographical risk exposure. Estonia, the UK and Germany were the top three countries to which the FIU made requests for information between 2015 and 2017 (see Table 8.2.). Regarding Russia though, the Finnish FIU indicated that, in some cases, co-operation was more efficient when directing the requests to investigative authorities directly.

⁸⁸ Tax authorities (presentation made during the onsite)

Table 8.30. FIU's international outgoing requests: top 10 countries (2015-17)

Country (outgoing)	
Estonia	80
UK	44
Germany	31
Latvia	30
Sweden	27
Poland	25
Turkey	24
Spain	21
Italy	17
Netherlands	17
Other (65 countries)	230
Total	546

Source: Finnish authorities

484. The FIU provides relevant information to its international counterparts and competent authorities, mainly on request. FATF delegations that have given feedback on their interaction with the Finnish FIU unanimously welcomed the quality and clarity of the information received, in particular on CFT-related cases. Between 2015 and 2017, the FIU received 241 international requests, mainly from Estonia, Russia and the United States.

Table 8.31. FIU's international incoming requests top 10 countries (2015/17)

Country (incoming)	
Estonia	20
Russian Federation	19
US	13
Netherlands	12
Belgium	11
Hungary	10
Luxembourg	9
Germany	8
Sweden	8
France	7
Other (53 countries)	124
Total	241

Source: Finnish authorities

485. The FIU also spontaneously disseminates information to foreign FIUs, and other competent authorities, but in a more limited way. The FIU sent 12 spontaneous international disseminations in 2015, 24 in 2016 and 21 in 2017. FATF delegations that have provided feedback on their interaction with the Finnish FIU mentioned

information spontaneously received in cases related to drug-related case, or payment card fraud.

486. *LEAs - The National Bureau of Investigation (NBI) and police forces in general, cooperate routinely with their foreign counterparts, formally and informally, to share information and conduct investigations. Although no comprehensive data is available on the outgoing requests formulated by Finnish police forces, the description of the investigation process and the several cases presented show that the international dimension is an integral part of the ML/TF approach of the police, including for example in many cases of wiretapping. This is confirmed by the volume of international information exchanges in ML cases described in Table 8.4, which only refers to co-operation with police offices from other EU Member States (Siena process). Russian LEA colleagues have proved efficient partners for investigations (see example in Box 8.5).*

Table 8.32. International information exchanges concerning ML (SIENA)

	2015	2016	2017
Sent	201	206	237
Received	630	535	626
Total	831	741	863

Source: Europol National Unit Finland Statistics

Box 8.30. Example of NBI cooperation with Russian authorities

The Finnish NBI and the Russian Federal Security Service (FSB) carried out parallel investigations in a case involving the sale of Russia property in Finland, under market value. The NBI initiated a criminal case for aggravated ML in order to determine if the seller of the property had laundered the assets resulting from the offence.

487. The Russian and Finnish investigators met regularly in Moscow (six meetings between 2014-2016 and continuous communication by phone and e-mail). MLA requests to Switzerland, where EUR 4.5 million had been transferred from Finland, were implemented mutually. During the investigation, four Russian investigators spent one week in Finland and attended interviews. Correspondingly, the Finnish investigators and prosecutor interviewed in Moscow the Russian suspect, who was convicted to a four-year imprisonment. The Finnish prosecutor is currently prosecuting the Finnish suspects primarily for aggravated fraud. The NBI has shared several examples of its participation in and initiation of joint investigations with other countries in ML and TF cases, especially with Estonia and other Nordic countries.

Box 8.31. Examples of NBI joint investigations

See Case Violet (Box 3.4) and Case Manse (Box 3.6).

Case Leopold –The predicate offences, mainly tax fraud were committed in Finland and the ML in Estonia. The case started when the NBI received a request to investigate a construction company. The workers came from Estonia and therefore a joint investigation team was started together with Estonia. In this case, the NBI has worked closely with the Finnish Tax Administration and the Estonian police and also cooperated with Europol and Eurojust.

488. The NBI can also count on the locally posted police and customs liaison officers, including Nordic countries' joint liaison officers or other EU liaison's officers, who have proved a useful resource to help build cases. The four Finnish Police liaison officers posted in Russia, as well as the two Customs officers also prove useful assets (and reciprocally, Russia has liaison officers stationed in Finland). NBI also referred to an Iraq liaison officer who helped in a TF case.

489. *Customs* - International co-operation is an integral part of Customs' ML/TF activities, especially for detecting and pursuing illicit cross-border cash transportation. Customs' strategy to combat financial crime, including AML/CFT, includes full and continuous co-operation with foreign counterparts and other relevant authorities (including FIUs, through the Finnish FIU if required). Customs develops a risk assessment for all its operations, which covers new trends (incl. for cash couriers), modus operandi, new hiding places etc. If and when relevant, third countries, and other relevant authorities, are invited to take part in Customs' operations based on these plans. To date, such operations have been conducted mainly with neighbouring countries, including Russia and Lithuania, although China, Singapore and Nigeria were also mentioned.

490. On the detection of and actions towards illicit cash couriers, Customs also conducts European joint operations.⁸⁹ These are conducted mainly with Baltic and Nordic countries. In addition, if there is suspicion, Customs sends risk information to other countries, mainly the Netherlands, Romania and Belgium so far.

491. *Tax authorities* - International co-operation is prioritised by tax authorities both to determine the target and scope of adequate preventive measures and to conduct tax-related investigations. As part of the Strategy on the Prevention of the Grey Economy and Economic Crime (see Chapter 1), Finland seeks to define the profile of potential tax offenders as specifically as possible. The Tax Administration has therefore proactively reached out to the relevant authorities of neighbouring countries, whose nationals or registered businesses were often found to be involved in tax-related offences in Finland. Targeted preventive measures have been determined, e.g. the introduction of the requirement of a tax number for construction workers, of particular relevance for Estonia (see IO.1). Administrative co-operation between Finnish and Estonian tax authorities has also been implemented, especially through the presence of tax officers in respective offices and

⁸⁹ Customs Co-operation Working Party (CCWP) of the Council of the European Union

participation in administrative enquiries (PAOE programme), to determine if Estonian companies have a permanent establishment in Finland and are therefore eligible for Finnish taxes.⁹⁰

492. Tax authorities also rely on international co-operation to conduct tax-related investigations, including those with ML connections.

Box 8.32. Example of tax authorities' international co-operation

*“Operation Tulipan Blanca”*⁹¹ - In April 2018, operation *Tulipan Blanca*, coordinated by Europol and conducted by the Spanish Guardia Civil with the support of Finnish authorities and the US Homeland Security Investigation, has seen 11 arrests and 137 individuals investigated. Members of a crime ring laundered money earned by their organized crime groups, who made their money selling drugs, by using credit cards and cryptocurrencies. The investigation showed that the suspects deposited more than EUR 8 million in cash, using 174 bank accounts.

Thanks to the collaboration with the Finnish authorities, it was established that the local bitcoin exchange was based in Finland and the Spanish Guardia civil could gather all the information on the suspects held by the cryptocurrency exchange.

493. *Supervisory bodies* - There is good international co-operation for the supervision of international financial institutions (FIs)/groups. Some of the largest FIs supervised by FIN-FSA are subsidiaries or branches of large Nordic groups. For such cross-border FIs, FIN-FSA discusses common supervisory issues with other Nordic supervisors. This was the case in recent years for the group supervision of the two largest credit institutions operating in Finland. This enables FIN-FSA to coordinate its activities and decide whether to focus on the same FIs as its Nordic colleagues. There is also good ad hoc co-operation and exchanges of information between Nordic supervisors when cross-border issues arise that might affect the whole group (e.g. Panama papers).

494. Outside the Nordic region, FIN-FSA attends EU AML/CFT supervisory colleges which have been formally established to assist in the supervision of specific cross-border FIs or groups. This was the case over the last years for one payment institution. Such colleges facilitated the sharing of experiences of ML/TF and AML/CFT issues in relation to such FIs.

495. FIN-FSA has cooperated with other supervisory authorities in the context of various cross-border cases related to ML. This happened in the Panama papers and the Russian laundromat cases, for which FIN-FSA contributed to the AML/CFT EU joint committee for the banking, securities and insurance supervisors (Anti Money Laundering Committee, AMLC).

⁹⁰ Tax authorities (presentation made during the onsite)

⁹¹ Tax authorities (presentation made during the onsite)

496. FIN-FSA's formal and informal interaction, meetings and exchanges of information with other AML/CFT supervisors, especially those in the Nordic region, are also key elements in the common understanding of ML/TF risks faced by the FIs under its supervisory remit. However, there could be an over-reliance on input collected through those channels. FIN-FSA should be encouraged to be more parochial and engage domestically with the RSAA and other DNFBP supervisors, to help build a joint and better picture of the ML/TF risks faced by the Finland-based FIs and DNFBPs in the Finnish ML/TF context, taking into account the national specificities and characteristics (see IO.3).

497. International co-operation of other supervisors is limited, in line with the domestic scope of the activities of these businesses and professions.

International exchange of basic and beneficial ownership information of legal persons and arrangements

8

498. Competent authorities are able to provide basic information on legal persons registered in Finland. The trade register is an open source, but given the concerns expressed on the accuracy of the information available (see IO.5), additional checks and collection of information are made by Finnish authorities receiving requests from international counterparts. For example, the FIU conducts extended searches and request information from private entities, or relevant authorities like the Tax Administration.

499. Finnish authorities provide information to their international counterparts on beneficial ownership (BO), but the timeframe to access and check the information can be long. In the absence of a centralised repository containing BO information in Finland (see IO.5 on the upcoming introduction of a national BO register), based on Finnish authorities' experience (e.g. the FIU), the timeliness with which BO information can be provided varies from a few hours to a few months. This depends on the complexity of the corporate structure, the numbers of entities involved, the international connections etc. Competent authorities use various sources of information: CDD information collected by obliged entities; cross-checking the register's information with other sources, reporting of the legal entity itself, compliance reports from the tax authorities etc.

500. There are no statistics on how often basic and BO information is requested by and provided to foreign countries. Finnish authorities estimate that it is more common for them to send requests to other countries (mainly to the neighbouring countries), than to receives such requests.

Overall conclusion on IO.2

501. **Finland has achieved a high level of effectiveness for IO.2.**

Technical Compliance Annex

Recommendation 1 – Assessing risks and applying a risk-based approach

These requirements were added to the FATF Recommendations when they were revised in 2012 and therefore were not assessed under the 3rd Round mutual evaluation of Finland, which occurred in 2007.

Criterion 1.1 – The Act on Preventing Money Laundering and Terrorist Financing 444/2017 (“AML/CFT Act”) requires the development of a national risk assessment (NRA) to identify and assess the money laundering and terrorist financing (ML/TF) risks in the country (Chapter 2, section 1). The identification of ML/TF risks has been conducted in 2014 (and published in 2015), in the form of a research project with the involvement of Finnish authorities and private sector entities, referred to as the National AML/CFT Risk Assessment 2015 (NRA 2015). On that basis, some areas have been listed as “key risks items” for ML/TF, constituting the NRA. However, this analysis does not reflect the nature and the level of the risks to which Finland is currently most exposed. A 2016/20 National Strategy on the Prevention of Grey Economy and on Economic Crime has also been developed, which includes an AML component, and an AML Action Plan was published in 2018, based on the NRA 2015. Finland also has a strategy on countering terrorism, which refers to TF. However, these strategic papers do not evidence that all Finnish authorities have comprehensively identified and assessed their ML/TF risks.

Criterion 1.2 – The Ministry of the Interior is in charge of coordination to assess ML/TF risks (AML/CFT Act, Chapter 2, section 1).

Criterion 1.3 – The AML/CFT Act requires that the NRA is updated on a regular basis (Chapter 2, section 1). The key risks items identified in 2014/15 have not been reviewed since then. In light of the steps taken by Finland to mitigate those risks, in particular through amendments brought to its AML/CFT legislative framework, the analysis is now outdated. The National Strategy on the Prevention of Grey Economy and Economic Crime covers the period 2016/20 and the strategy on terrorism has been updated in 2016.

Criterion 1.4 – The Ministry of the Interior is required to publish a summary of the NRA (AML/CFT Act, Chapter 2, section 1). The regular communication channels with competent authorities, self-regulatory bodies (SRBs) and obliged entities were used to provide information on the result of the NRA 2015.

Criterion 1.5 – One of the purposes of the NRA is to support and reinforce the allocation of resources and the fight against ML and TF (AML/CFT Act, Chapter 2, section 1). However, the lack of a comprehensive and updated identification and assessment of ML/TF risks by Finnish authorities (cf. c. 1.1) limits the ability to allocate resources based on risks and implement appropriate prevention and mitigation measures at national level.

Criterion 1.6 –

(a) Electronic money transactions are exempted from customer due diligence (CDD) requirements, provided that the associated ML/TF risks are low, the exemption occurs in strictly limited and justified circumstances and it relates to a particular type of financial activity (AML/CFT Act, Chapter 3, Section 9).

(b) The AML/CFT Act is not applicable to financial activities if they are conducted on an occasional and very limited basis, accounting for no more than 5% of the turnover in any accounting period, and with a EUR 1 000 threshold for each individual transaction (Decree 678/2017), and do not include money remittances activities (AML/CFT Act, Chapter 1, section 3, subsection 1).

Criterion 1.7 – Obligated entities are required to apply enhanced due diligence (EDD) measures when they identify high risks in their risk assessment (AML/CFT Act, Chapter 3, section 10), and to have in place policies, procedures and controls sufficient to reduce and effectively manage the risks (AML/CFT Act, Chapter 2, section 3, subsection 2).

Criterion 1.8 – The AML/CFT Act allows obliged entities to apply simplified due diligence measures (SDD) when ML/TF risks are “negligible”, based on their risk assessment (Chapter 3, section 8, subsection 1).⁹²

Criterion 1.9 – Obligated entities are required to communicate their risk assessment and changes brought to them without undue delay to supervisors (AML/CFT Act, Chapter 2, Section 3). They are also expected to demonstrate to supervisors that CDD and monitoring processes are adequate in view of their ML/TF risks (Chapter 3, Section 1), and can be sanctioned for failure to comply with these obligations (Chapter 8, Sections 1 and 3).

Criterion 1.10 –

(a) The AML/CFT Act requires obliged entities to conduct a risk assessment (Chapter 2, section 3, subsection 1).

(b) When preparing their risk assessment, obliged entities are required to take into consideration the nature, size and extent of their activities (AML/CFT Act, Chapter 2, section 3, subsection 1). The Explanatory Memorandum (see Chapter 1) to the AML/CFT Act states that customers, countries and geographical regions, products and channels of distribution should especially be taken into account.

(c) Obligated entities should update their risk assessment on a regular basis (AML/CFT Act, Chapter 2 section 3, subsection 1).

(d) Obligated entities’ risk assessments and changes brought to them should be communicated without undue delay to supervisors (AML/CFT Act, Chapter 2, Section 3).

⁹² A government decree, under consideration, will define factors indicating situations when the risks can be viewed as “negligible” (Chapter 3, section 8, subsection 2).

Criterion 1.11 –

(a) Obligated entities are required to have in place policies, procedures and controls, approved by senior management, that are sufficient to reduce and effectively manage their ML/TF risks (AML/CFT Act, Chapter 2, section 3).

(b) Obligated entities are required to monitor, and if required enhance, applicable mitigation measures (AML/CFT Act, Chapter 2 section 3).

(c) Obligated entities are required to apply EDD measures when they identify high risks in their risk assessment (AML/CFT Act, Chapter 3, section 10), and to have in place policies, procedures and controls sufficient to reduce and effectively manage the risks (AML/CFT Act, Chapter 2, section 3, subsection 2).

Criterion 1.12 – The AML/CFT Act allows obliged entities to apply simplified due diligence measures (SDD) when ML/TF risks are “negligible”, on the basis of their risk assessment (Chapter 3, section 8) (see c.1.8).⁹³ Customers must be identified in all cases of suspicious transactions (AML/CFT Act Chapter 3, section 2, subsection 3), but there is no exemption from SDD measures when there is a suspicion of ML/TF.

Weighting and conclusion: The deficiencies identified in Finland’s identification and assessment of its current ML/TF risks have a strong impact on the rating.

Recommendation 1 is rated largely compliant.

Recommendation 2 – National cooperation and coordination

In its 3rd MER, Finland was rated largely compliant with these requirements (para.701-713). The main deficiencies related to the effectiveness of inter-agency cooperation targeting ML/TF specifically and limited feedback between agencies with respect to investigations and results of inter-agency disseminations. R. 2 is now more specific about the need for countries to have national AML/CFT policies that encompass identified risks and for coordination to be more formalised.

Criterion 2.1 – One of the purposes of the NRA is to support the preparation of consistent policies for combating ML/TF (AML/CFT Act, Chapter 2, section 1). Some legislative measures have been taken, including in the 2017/18 AML/CFT Act, to address some of the key risks identified in the NRA 2015 (see c.1.1.), and an Action Plan of Public Authorities for Enhancing the Prevention of ML was adopted in June 2018. However, the Action Plan is based mainly on the 2015 key risks that are outdated. No similar approach was taken for TF.

Criterion 2.2 – The FATF Steering group, chaired by the Police department of the Ministry of the Interior, is in charge of ensuring the cooperation and coordination between national authorities for the prevention of ML/TF and the development of action plans against ML and TF (2015 Decision SMDno-2014-2798 of the Minister of the Interior).

⁹³ A government decree, still under consideration at the end of the onsite visit, will define factors indicating situations when the risks can be viewed as “negligible” (Chapter 3, section 8, subsection 2).

Criterion 2.3 – The FATF Steering group includes representatives of all public ministries and other relevant authorities involved in AML/CFT (2015 Decision). Nevertheless, a number of relevant authorities should be part of the Steering group on a permanent basis (ex. Tax administration, Patent and Registration Office, Åland authorities). The cooperation and coordination work of the Steering group focuses on the policymaking level. The National Coordination Group on Combating ML and TF was set up in May 2018 with a view to provide a platform for coordination between the FIU, supervisors and law enforcement authorities. Its main task is to improve the flow of information between supervisors and operational, law enforcement authorities and to harmonize the procedures for AML/CFT supervision.

Criterion 2.4 – The FATF Steering group is in charge of coordinating questions relating to the financing of the proliferation of weapons of mass destruction (PF) (2015 Decision SMDno-2014-2798). The Ministry of Foreign Affairs (MFA) is the competent authority for PF-related issues, with the Unit for Arms Control responsible for non-proliferation and the Unit for Public International Law responsible for sanctions, including PF-sanctions (MFA Rules of procedures and Act on Act on the enforcement of certain obligations of Finland as a UN and EU Member, Section 2b, Subsection 4).

Weighting and conclusion: Finland does not have comprehensive national AML/CFT policies based on an updated analysis of ML/TF risks, which is one of the main elements for this Recommendation.

Recommendation 2 is rated partially compliant.

Recommendation 3 – Money Laundering Offence

In its 3rd MER, Finland was rated partially compliant, as its ML offence did not cover all physical elements of the crime. It was not possible to prosecute for self-laundering, nor to prosecute for ML any person living in a joint household with the offender, and there was no offence for conspiracy available for the ML basic offence.

Criterion 3.1 – The Finnish ML provisions meet many of the requirements set by the *Vienna* and *Palermo Conventions* (Criminal Code (CC), Chapter 32, sections 6 to 9) but some provisions are not fully in line. The ML offence does not cover the acquisition, possession and use of property when the perpetrator does not intend to conceal or obliterate the illegal origin of such proceeds or property or to assist the offender in evading the legal consequences of the offence or in order to obtain benefit for himself or for another. This is not consistent with Art. 6(1)(b)(i) of the Palermo Convention nor with Art. 3(1)(c) of the Vienna Convention which do not require an intentional element to conceal or obliterate the illegal origin for the mere acquisition, possession and use of property which is the proceeds of crime. This deficiency is partly limited in Finland by the fact that ML offences are also punishable when committed with gross negligence (CC, Chapter 32, Section 9) where intentionality does not need to be established. The receiving offences (CC, Chapter 32, Section 1-5) do cover possession and acquisition, and do not require the intentional element, but apply only with respect to “*theft, embezzlement, robbery, extortion, fraud, usury or means of payment fraud*”. Thus, the possession of proceeds of crime and the acquisition or use of such property is not criminalised in all cases.

Finally, the ML offence does not apply to a person living in a joint household with the offender, and who only used or consumed property obtained by the offender for ordinary needs in the joint household (CC, Chapter 32, Section 11(2)). This limitation remains very narrow, based on reasons of equity and concern – according to the preparatory legislative work, the “use and consumption” for “ordinary” needs in the joint household- This limited scope has been confirmed by a Supreme Court judgment in 2009.

Criterion 3.2. – Any offence can be a predicate offence for ML in Finland (CC, Chapter 32, Sections 6-11) and the Criminal Code criminalises all designated categories of offences.

Criterion 3.3. Finland does not apply a threshold approach and all categories of offences can be predicate offences for ML.

Criterion 3.4. – The ML offence extends to any type of property, regardless of its value, that directly or indirectly represents the proceeds of crime (CC, Chapter 32, Section 6).

Criterion 3.5. – When proving that property is the proceeds of crime, it is not necessary that a person be convicted of a predicate offence. There is no provision in the CC making it necessary, and this is confirmed by the Explanatory Memorandum (see Chapter 1) HE 53/2002.

Criterion 3.6. – ML is punishable in Finland when the predicate offence is punishable in the State where it was committed. Finland has extraterritorial criminal law jurisdiction and dual criminality is required unless the predicate offence is a serious offence (CC, Chapter 1, Sections 10 and 11). Applying Finnish criminal law to offences committed in the territory of a foreign State requires, as a main rule, that the act is also punishable under the law of the place of commission and that a sentence could have passed for the offence by a court of that State. However, there are also many exceptions to the dual criminality requirement as concerns international offences and other serious offences (CC, Chapter 1, Section 11 (2), and Section 7).

Criterion 3.7 – Self-laundering is criminalised as a separate offence from the predicate offence only in circumstances where the conduct would be considered to constitute aggravated ML, and when the ML offence prevails over the predicate offence (CC, Chapter 32, Section 11). Regarding other self-laundering cases, Finland authorities state that it is a fundamental principle in the Finnish criminal law system that the punishment for the offences that yield property covers actions by which the perpetrator exploits or secures the property. This includes actions that would constitute ML offences. Therefore punishing cumulatively for the predicate offence and for ML would – according to Finland - violate the *ne bis in idem* rule (double jeopardy principle), which is a constitutional fundamental right in the Finnish legal system (Constitution of Finland, Section 22; European Convention on Human Rights, Protocol No. 7, Article 4). This topic was extensively discussed between the assessment team and the Finnish authorities during the 3rd Round mutual evaluation of Finland and the follow-up process, supported by comprehensive legal analysis.⁹⁴ The conclusion was that fundamental principles of domestic law were not present, and

⁹⁴ 2007 MER of Finland; 2012 6th Follow-up Report; 2013 Exit from regular FUR

that Finland referred rather to legal concepts (or legal constraints) which form the basis for the criminalisation of criminal conduct, including ML. Finland does not bring new elements that would justify a different approach and conclusion. The fact that self-laundering is criminalised in specific circumstances is in any case an indication that there are no fundamental principles of domestic law that would prevent the criminalisation of self-laundering, and consequently there seems to be no reasonable justification for the limited scope of the self-laundering provision.

Criterion 3.8 – There are no restrictions in the Finnish legislation regarding the possibility to take into account objective factual circumstances when intent and knowledge are to be demonstrated (Code of Judicial Procedure, Chapter 17, Section 1 on the rule of free consideration of the evidence).

Criterion 3.9 – The maximum penalty for “normal” ML and negligent ML is two years’ imprisonment *or* a fine (CC, Chapter 32, Section 6); for aggravated ML, at least four months and at most six years of imprisonment (Section 7); for conspiracy for the commission of aggravated ML, a fine *or* one year of imprisonment at most, but only in those instances in which the proceeds are derived from bribery, aggravated EU tax fraud or aggravated subsidy fraud (Section 8). For ML violation (if the ML or the negligent ML is petty, CC, Section 32, Section 10), the maximum penalty is a fine. The maximum punishment for aggravated ML (six years) is higher than the standard of four years for most aggravated offences in the CC, and if conditional imprisonment by itself is to be deemed an insufficient punishment for the offence, ancillary fines might be imposed (CC, Chapter 6, Section 10). However, fine and imprisonment cannot be cumulated for ML, negligent ML. These elements affect the full proportionality of sanctions.

Criterion 3.10 – Criminal liability and sanctions for legal persons are provided for (CC, Chapter 32, Section 14, in connection with CC, Chapter 9), and they are without prejudice to the criminal liability of natural persons (CC, Chapter 9, Section 2(2) mentioning that a corporate fine may be imposed even if the offender cannot be identified or otherwise is not punished). The criminal liability does not exclude other liability and parallel proceedings. The criminal fine ranges between EUR 850 and EUR 850.000. The provisions on corporate liability apply to ML, aggravated ML and negligent ML (CC, Chapter 32, Section 14). However, they do not apply to ML violation, neither to conspiracy for basic ML offence. Other types of sanctions, including civil and administrative, are provided by different legal vehicles (Act of the FSA, Act on Payment institutions, on Credit institutions, Investments services, etc.)

Criterion 3.11 – There are appropriate ancillary offences to the ML offence, including attempt (CC, Chapter 32, section 6 and 7), complicity (Chapter 5, section 3), commission via agent (Chapter 5, section 4), instigation (Chapter 5, section 5). However, conspiracy is not punishable in relation to the ML offence (only aggravated offence, see c. 3.1) but the scope of this deficiency is relatively narrow. In addition, aiding and abetting are not fully covered since an accomplice in the predicate offence cannot be sentenced for ML, even though this person may be sentenced for an aggravated ML offence if this offence “*with consideration to the continuous and planned nature of the acts, forms the essential and blameworthy part of the totality of offences*” (CC, Chapter 32, Section 11(1)).

Weighting and conclusion: The main shortcomings include the definition of ML which requires an intentional intent which is not fully consistent with the Vienna

and Palermo Conventions; the criminalisation of self-laundering which is limited to aggravated ML. Conspiracy is also limited to aggravated ML.

Recommendation 3 is rated largely compliant.

Recommendation 4 – Confiscation and Provisional Measures

In its 3rd MER, Finland was rated largely compliant. The main shortcoming was that it was not possible to confiscate property of value corresponding to the laundered proceeds.

Criterion 4.1 – Provisions of Chapter 10 of the CC organise the general confiscation regime in Finland, and specific provisions apply to confiscation in case of ML, aggravated and negligent offences (CC, Chapter 32).

(a) Property that has been the “target of” (property laundered) a ML offence, aggravated ML and negligent ML is subject to be forfeited to the State (CC, Chapter 32, Section 12 (1) which refers to offences targeted in Sections 6, 7 and 9).

The general provisions of the CC on confiscation require that an act criminalised by law (offence) has been committed (CC, Chapter 10, Section 1 (1)). Therefore, ML Violation (Section 10) and conspiracy for aggravated ML (Section 8) are also potentially subject to confiscation under those general provisions (CC, Chapter 10). These provisions also cover property held by third parties (CC, Chapter 10, Section 2 (1)). Deficiencies identified in R.3 as regard the scope of the ML offence have a limited impact on this sub-criterion.

(b) Proceeds of crime are subject to confiscation, and the general confiscation regime targets the “perpetrator, a participant or a person on whose behalf or to whose benefit the offence has been committed”, where these have benefited from the offence (CC, Chapter 10, Section 2). This applies to all ML and TF offences in the Criminal Code. Income and other benefits can be confiscated as proceeds of crime (CC, Chapter 10, Section 2 and 3).

Instrumentalities are also subject to confiscation if used in the commission of an offence or intentional offence or closely connected to an intentional offence (CC, Chapter 10, Section 4). Confiscation of instrumentalities therefore requires that an offence has been committed and that the offence and the property to be confiscated are closely connected. This criterion requires that an instrumentality intended for use (and not used yet) should also be subject to confiscation. Instrumentalities closely connected to an intentional offence but not used under the particular case or due to the inchoateness of the offence (e.g. an attempt or conspiracy of a ML or TF offence), can be confiscated. Furthermore, instrumentalities can be confiscated even if there is no conviction of the offence if proceedings have been brought for the offence.

(c) Confiscation applies to any act criminalized by law (CC, Chapter 10), which therefore includes TF, terrorist acts or terrorist organizations.

(d) Under the general confiscation provisions of the CC, Chapter 10, Section 2 (see c. 4.1(a)), confiscation applies to the proceeds and corresponding value of the property derived from crime. In addition, the value of instrumentalities can be confiscated even if the instrumentalities themselves cannot be confiscated (Section 8). As concerns the property that has been “target of the” (i.e. property laundered) ML,

aggravated ML, and negligent ML, confiscation is organised by Chapter 32, Section 12 of the CC, and there is no value-based confiscation provided. Therefore, in these cases, corresponding value of property can only be confiscated proceeds of the predicate offence, and not as property laundered in a standalone or third party ML investigation. The extended confiscation (CC, Chapter 10, Section 3) facilitates confiscation of proceeds of crimes without the need to demonstrate that the proceeds are derived from the predicate offence. However, this is not a substitute for value-based confiscation, as this does not apply to all ML offences (and to negligent ML) and applicable provisions still require that consideration needs to be given as to whether or not the property is “clearly derived from criminal activity that is not considered insignificant”.

Criterion 4.2 –

(a) The identification, tracing and evaluation of property subject to confiscation can be done at the time of criminal investigations either through investigative measures or through measures taken by the district bailiffs under the Enforcement Code, on the basis of a freezing order issued by a district court or a temporary freezing order given by the police or prosecutor. The district bailiffs have the right to disclose information to the prosecutors and investigative authorities for the purposes of investigation and prosecution and court proceedings, as well as for the prevention of serious criminal offences (Enforcement Code, Chapter 3, section 70).

(b) Provisional measures can be carried out to prevent any dealing, transfer of disposal of property subject to confiscation, including a freezing order (by a district court) and a temporary freezing order that may be given by a senior ranking police officer or prosecutor (Coercive Measures Act, Chapter 6).

(c) Competent authorities can take steps that will prevent or void actions that prejudice Finland’s ability to freeze or seize or recover property that is subject to confiscations: extended confiscation and confiscation of value (CC, Chapter 10, Section 8). If an object or property referred to in Section 4 (instruments) or 5 (certain other property) cannot be ordered forfeit owing to a restriction, or because the object or property has been hidden or is otherwise inaccessible, a full or partial forfeiture of the value of the object or property may be ordered. There is also a possibility to conduct confiscation proceedings in the absence of the defendant (CC, Chapter 10 Section 9). Interim freezing (Coercive Measures Act, Chapter 6 section 3) is also possible. Finally, an appeal against seizure and freezing does not suspend the seizure or freezing (Coercive Measures Act, Chapter 10 - Confiscation for Security - and Section 9 - Appeal).

(d) The Criminal Investigations Act is of general application to any criminal offences, including money laundering and terrorist financing (see R. 31).

Criterion 4.3 – Rights of *bona fide* third parties are protected under the “general” confiscation regime (CC, Chapter 10, Section 2, 6, 11 (1), and for appeal, Coercive Measures Act, Chapter 6, Section 9, Chapter 7). The same protection applies with respect to confiscation connected to ML, aggravated and negligent offence (CC, Chapter 32).

Criterion 4.4 – There are legislative measures applicable to the management and disposition of property frozen, seized or confiscated, including assets, funds, chattels, real estate and property at large (Coercive Measures Act, Chapters 6

(Section 10) and 7 (Section 13); Enforcement Code (Chapters 6 and 8). These provisions include precautionary measures to be taken for perishable or income generating assets.

Weighting and conclusion: Deficiencies identified in R. 3, and to a lesser extent in R. 5 have an impact on the level of compliance of R. 4. Deficiencies are noted in the confiscation of corresponding value of property laundered for ML, aggravated ML, and negligent ML.

Recommendation 4 is rated largely compliant.

Recommendation 5 – Terrorist Financing Offence

In its 3rd MER, Finland was rated largely compliant on these requirements. The main shortcoming was that funding a terrorist or a terrorist organisation without a specific link to a terrorist act was not publishable.

Criterion 5.1 – The offences mentioned in the CC (Chapter 34(a), Sections 5(1) cover those listed in the annex to the Terrorist Financing Convention, and apply to any person who directly or indirectly provides or collects funds in order to finance, or aware that these shall finance such offences. This is consistent with Article 2 of the Convention.

Criterion 5.2 –

(a) A person who directly or indirectly provides or collects funds in order to finance or aware that these funds are used (CC, Chapter 34(a), Section 5(2)) to finance an offence made with terrorist intent; to prepare an offence to be committed with terrorist intent; to direct a terrorist group; to promote the activity of a terrorist group (CC, Chapter 34(a), Sections 1-4), or to provide training for the commission of a terrorist offence; to train for the commission of a terrorist offence; or to recruit for the commission of a terrorist offence (Sections 4(a) – 4 (c)); or travel for the purpose of committing a terrorist offence (Section 5(b)) shall be sentenced for the financing of terrorism.

(b) A person, who directly or indirectly gives or collects funds for a terrorist group (defined in CC, Chapter 34(a), Section 6(2)), and aware of the nature of the group as a terrorist group, shall be sentenced for financing of a terrorist group (Chapter 34(a), Section 5(a)). No link to specific terrorist act or acts is required in that regard. As regards the financing of an individual terrorist, there is no explicit provision in the CC. However, since the offences of Chapter 34(a), Sections 5(2) (see above c.5.2 a) are consistent with the definition of *Terrorist* of the FATF Glossary and do not only include offences made with terrorist intent, any person committing or attempting to commit one of these offences would therefore be considered as a terrorist in Finland. However, Section 5(2) still requires a link to be made with the financing of these specific offences, even though the Explanatory Memorandum (see Chapter 1, 1.2.4) HE 18/2014 does not require that it is to be determined in detail, for example the time and the place of the act. It is therefore not clear if a court could condemn someone providing funds that would be used by an individual terrorist for any other purpose than committing or attempting to commit one of the offences included in Section 5(2).

Criterion 5.2 bis - TF offence extends to travelling for the commission of a terrorist offence and is applicable to a Finnish citizen or a person deemed equivalent to a Finnish citizen or a person travelling from the territory of Finland who travels to a state other than his or her residence or nationality to commit there a TF offence (CC, Chapter 34(a), Section 5(b)).

Criterion 5.3 - The definition of “funds” in Article 1(1) of the Terrorist Financing Convention applies in Finland as law, as according to Section 1 of the Act (law 558/2002) which ratified the TF Convention, provisions of the Convention belonging to the field of legislation are in force as a law. This covers Article 1(1) of the Convention.

Criterion 5.4 -

(a) Finland’s provisions regarding financing of terrorism (CC, Chapter 34(a)) would not require that the funds were actually used to carry out or attempt a terrorist act.

(b) As highlighted in c.5.2 b), Section 5(2) of the CC requires that a link is made between the funding provided and the specific offences of Sections 1-4 and Sections 4(a)-(c) for TF offence.

Criterion 5.5 - There are no restrictions in the Finnish legislation regarding the possibility to take into account objective factual circumstances when intent and knowledge are to be demonstrated (Code of Judicial Procedure, Chapter 17, Section 1 on the rule of free consideration of the evidence).

Criterion 5.6 - Sanctions for TF are not fully proportionate nor dissuasive. The fact that the CC contemplates the possibility of sentencing by a fine or imprisonment of at most three years for the financing of a terrorist group offence is not proportionate neither with the TF offence (minimum sanction is imprisonment for at most four months, maximum eight years) nor with other serious criminal offences, including the terrorist offence, that are punished only by imprisonment (Chapter 34(a), Sections 5(1) and (2)). Moreover, the maximum sanction for financing a terrorist group (3 years) is not proportionate with the maximum sanction for TF (at most 8 years); neither it is dissuasive, as per the minimum sanction for TF (4 months), even if this is proportionate with minimum sanctions for offences made with terrorist intent (Chapter 34a) Section 1).

Criterion 5.7 - Criminal liability and sanctions can be applied to legal persons. The provisions on corporate criminal liability apply to the TF offences (CC, Chapter 34(a), Section 8(1)). The criminal liability does not exclude other liability and parallel proceedings. The range of fines appear to be dissuasive, a corporate fine is at least EUR 850 and at most EUR 850 000 (CC, Chapter 9, Section 5). Other types of sanctions, including civil and administrative, are provided by different legal vehicles (Act of the FSA, Act on Payment institutions, on Credit institutions, Investments services, etc.); Even without a specific provision, the liability of legal persons is separate from the liability of natural persons. This is reflected by the Chapter 9, Section 2(2) of the Criminal Code mentioning that a corporate fine may be imposed even if the offender cannot be identified or otherwise is not punished.

Criterion 5.8 -

(a) Attempts to commit financing of terrorism are punishable (CC, Chapter 34(a), sections 5(3) and 5(a)(2)).

(b) Complicity in financing of terrorism is punishable (CC, Chapter 5, section 3). Complicity in an attempted offence is also punishable.

(c) “Organising” or “directing other to commit” TF offences would be covered by the provisions regarding instigation (CC, Chapter 5, Section 5) and abetting (CC, Chapter 5, Section 6).

(d) Participation in the activity of an organised criminal group is criminalised (CC, Chapter 17, section 1(a)). This provision covers cases where the aim of the group is to commit a serious offence of a certain degree, for example financing of terrorism (CC, Chapter 6, section 5(2)).

Criterion 5.9 – TF offences are designated as ML predicate offences (see 3.2).

Criterion 5.10 – The TF offences of the Criminal Code (Chapter 34(a)) are international offences (CC, Chapter 1, Section 7(3)). Finnish law applies to offences referred to in that chapter, regardless of the law of the place of commission. This means that the Finnish law is applicable in all cases and financing of terrorism is covered by the jurisdiction of Finland regardless of the offender and the place of the commission of offence or other circumstances mentioned in Chapter 1 of the Criminal Code as a ground for application of Finnish criminal law. Dual criminality is not needed.

Weighting and conclusion: Finland has some minor shortcomings. These include the fact that the TF offence for an individual terrorist requires that the funds are used to finance a specific terrorist offence, and that sanctions for TF are not fully proportionate nor dissuasive.

Recommendation 5 is rated largely compliant.

Recommendation 6 – Targeted Financial Sanctions related to Terrorism and Terrorist Financing

In its 2007 MER, Finland was rated partially compliant on those requirements, and major shortcomings were the lack of a national mechanism to consider requests for freezing from other countries or to freeze the funds of EU internals. In its 2013 9th FUR, Finland was still rated partially compliant.

Criterion 6.1 – (a)-(e)

At the EU level, Finland implements UNSCR 1267/1988 (on Afghanistan) through EU Regulation 753/2011 and Council Decision 2011/486/CFSP, and UNSCR 1267/1989 (on Al Qaida) through EU Regulation 881/2002 (and successors) and Common Position 2002/402/CFSP. These Regulations have direct legal effect in Finland.

At national level, the *Act on the Freezing of Funds with a View to Combating Terrorism* (“Freezing Act”), referred to by Finland as the relevant applicable legislation, explicitly lays down provisions for the implementation of UNSCR 1373 (Section 1) (see below c. 6.2 for detailed analysis), but not 1267/1989 and 1988 sanctions’ regimes. However, in practice persons and entities designated under UNSCR 1267/1989 would - in almost all cases - also meet the criteria under the Freezing Act which refers to acts criminalized in Chapter 34(a) of the Criminal Code (including *inter alia* directing of a terrorist group, promotion of the activity of a terrorist group, recruitment for the commission of a terrorist offence and financing of a terrorist

group). In these cases where the person or entity suspected of, charged with or convicted of such a crime is linked to ISIL or al-Qaeda, the listing criteria of 1267 sanctions regime can be met and the mechanism for designation as described in the Freezing Act (see below c.6.2) would apply. In other, cases, the MFA, by virtue of the Section 2(b) of the *Act on the Fulfilment of Certain Obligations of Finland as a member of the UN and EU, would be the authority “responsible for the duties imposed [...] by EU regulation[...], and by resolutions on the sanctions adopted by the UNSC [...].*

Criterion 6.2 – As an EU Member State, Finland implements UNSCR 1373 via the EU framework under Council Common Position (CP) 2001/930/CFSP, 2001/931/CFSP and EC Regulation 2580/2001. At national level, the Freezing Act establishes national mechanism implementing UNSCR 1373 (Section 1).

(a) *At the EU level*, the Council of the EU is the competent authority for making EU designations in order to implement UNSCR 1373. This is prepared by the COMET Working Party of the Council of the EU, which applies designation criteria consistent with the designation criteria in UNSCR 1373. Persons, groups or entities can be included on the list on the basis of proposals submitted by the EU Member States or third countries. *At national level*, under the Freezing Act, the NBI and the FIU have responsibilities regarding the proposals to freeze funds and the effective freezing of funds (Freezing Act, Section 4; FIU Act, Section 2 subsection 1 (7) which refers to the Freezing Act). The NBI maintains a public list of decisions to freeze funds (Section 8) and the Ministry of Foreign Affairs (MFA) is in charge of informing the UN Sanction Committee or the EU of the relevant freezing decisions (Section 9).

(b) *At the EU level*, the COMET Working Party of the Council of the EU applies designation criteria consistent with the designation criteria in UNSCR 1373 (see c.6.1a)).

At national level, there is a mechanism for identifying targets for freezing of funds. The FIU is responsible for establishing grounds for the decisions to freeze funds and for making proposals for decisions to freeze funds to the NBI (Freezing Act, section 4; FIU Act, section 2). A police officer with the power of arrest or a prosecutor shall report any suspicion or conviction meeting the designation criteria to the FIU operating within the NBI that will ultimately take the freezing decision (Freezing Act, Section 3)

(c) *At the EU level*, requests are received and examined by the Working Party on restrictive measures to combat terrorism (COMET). All Council working parties consist of representatives of the governments of the Member States. EU designations are directly effective in all EU Member States and must include sufficient identifying information to exclude those with similar names.

At the national level, when receiving an individualised and reasoned request, funds of the suspects will be frozen by Finland, if the requesting State has, on the basis of credible evidence, initiated a criminal investigation concerning the person or demanded the conviction of the person for an act which, if committed in Finland, would obviously have the essential elements of a terrorist offence or if a court in the requesting State has convicted the person of a terrorist offence (Freezing Act, Section 3(3), this provision refers to Chapter 34(a) of the CC on terrorist offences, which includes TF offence, see R. 5). This threshold to examine and give effect to

foreign freezing requests goes beyond “*whether reasonable grounds or a reasonable basis exists to initiate a freezing action*” as requested.

(d) *At the EU level*, the COMET Working Party uses a “reasonable basis” evidentiary standard, and designation is not conditional on the existence of criminal proceedings. EU designations under (CP) 2001/930/CFSP, 2001/931/CFSP and Regulation 2580/2001 are based on a decision in respect of the persons, groups and entities concerned, irrespective of whether it concerns the instigation of investigations or prosecution for a terrorist act, an attempt to perpetrate, participate in or facilitate such an act based on serious and credible evidence or clues, or condemnation for such deeds (CP 2001/931/CFSP, Article 1(4)). *At the national level*, funds belonging to a natural or a legal person who is reasonably suspected of, charged with or convicted of a terrorist act shall be frozen (Freezing Act, Section 3(2)). Requests from another country are conditional upon the existence of a criminal investigation, which goes beyond “*reasonable grounds*” (Freezing Act, Section 3, (3)).

(e) The MFA shall inform the competent international actors about a relevant decision to freeze funds made under section 3(1)(2) and (4 to 6) of the Freezing Act, stating the reasons for the decision. In accordance with the Personal Data Act, personal data may be transferred to outside the EU if the transfer is necessary for securing an important public interest (Personal Data Act, Chapter 5, Section 23, Subsection 5).

Criterion 6.3 – The deficiency of c.6.1 as regards the lack of a clear legal basis for implementation of UNSCR 1267/1989 and 1988 has some effect on this criterion.

(a) *At EU level*, all Member States are required to provide each other with the widest possible range of police and judicial assistance in matters related to persons/entities that meet the criteria for designation, inform each other of any measures taken, and cooperate and supply information to the relevant UN Sanctions Committee. *At national level*, the FIU is in charge of establishing grounds for the decision to freeze funds, and making proposals for decisions to freeze funds (Freezing Act, Section 3 (2) and 4; FIU Act, Section 4). The FIU has a right to obtain information necessary to detect terrorist financing notwithstanding the provisions on the secrecy of information (FIU Act, Section 4). Information used to identify natural or legal persons that meet the criteria laid down in the Freezing Act is collected by intelligence and law enforcement authorities. A police officer with the power of arrest or a prosecutor shall report to FIU any suspicion or conviction of natural or legal persons reasonably suspected of, charged with or convicted of a terrorist offence (Freezing Act, Section 3).

(b) *At the EU level*, designations take place without prior notice to the person/entity identified (Art. 7a(1) Regulation 881/2002 and EC Regulation 1286/2009 preamble para.5). For asset freezing, the Court of Justice of the EU makes an exception to the general rule that notice must be given before the decision is taken in order not to compromise the effect of the first freezing order. The listed individual or entity has the right to appeal against the listing decision in Court, and seek to have the listing annulled. *At national level*, competent authorities have legal authority and procedures or mechanism to operate ex parte against a person whose freezing of assets is envisaged. There is no explicit provision for this but decisions to freeze funds take effect without a prior notice in case of both national freezing decisions

and EU designations (Freezing Act, Section 4, Subsection 3; Section 14, Subsection 2).

Criterion 6.4 –

At the EU level, implementation of TFS, pursuant to UNSCRs 1267/1989 and 1988, does not occur “without delay.” Because of the time taken to consult between European Commission departments and translate the designation into all official EU languages, there is often a delay between when the designation and freezing decision is issued by the UN and when it is transposed into EU law under Regulation 881/2002. An expedited procedure has been adopted by the Commission for implementation of new listings required by for UNSCR 1989 transposed under EU Regulation 881/2002. The delay between the date of designation by the UN and the date of its transposition into EU framework has consequently shortened to an average of 3-4 days in 2016 and 2017. This is still not consistent with the requirement to implement sanctions “without delay”. For resolution 1373, TFS are implemented without delay because, once the decision to freeze has been taken, Council Regulation 2580/2001 is immediately applicable to all EU Member States.

At national level, Finland has legal provisions that would enable it to implement without delay UNSCR obligations directly by decree, without relying on the EU implementation process (Act on the fulfilment of certain obligations of Finland as a Member of the United Nations and of the European Union, “Sanctions Act”). As far as designations in order to implement UNSCR 1373 are concerned, Council Regulation 2580/2001 is directly applicable within the EU. The designation enters into force on the day of its publication. Similarly, the decisions to freeze funds in accordance with the Freezing Act takes effect on the day of publication in the Official Gazette and are to be implemented immediately regardless of appeal (Freezing Act, Section 4, as confirmed in the Explanatory Memorandum (see Chapter 1).

Criterion 6.5 – All natural and legal persons are directly under the obligation to freeze funds of designated persons and entities (EU regulations; Freezing Act, Section 14). The competent authority for implementing and enforcing freezing of property and assets is the district bailiff of the Special Enforcement Unit in Helsinki (Freezing Act, Section 14; Sanctions Act, Section 2b). The bailiff is an enforcement officer who acts under the instructions and responsibility of local enforcement authorities, such as the Helsinki enforcement office. The Enforcement Code (705/2007) lays down the procedure for enforcement (of judicial decisions) and the competencies of the enforcement authorities.

(a) For UNSCRs 1267/1989 and 1988, EU regulations transposing UNSC decisions are directly applicable in all EU Member States on the day of publication in the EU’s Official Journal. There is an obligation on all natural and legal persons to freeze all funds, financial assets, or economic resources of all designated persons and entities (irrespective of their nationality) (EC Regulations 881/2002 art. 2(1), 1286/2009 art. 1(2), 753/2011 art.3, 754/2011 art.1). However, the delays noted above in transposing UN designations into EU Regulations can result in de facto prior notice to the persons or entities in question.

For UNSCR 1373, the obligation for natural and legal persons to freeze the assets of designated persons derives automatically from the entry into force of EU regulation, without any delay and without notice to the designated individuals and entities

(EC Regulation 2580/2001 art. 2(1a)). In Finland, EU internals are covered by the Freezing Act (Section 3, Subsection 1) which provides that the funds/assets of a natural or legal person listed under Council CP 931/2001/CFSP and not covered by EC Regulation 2580/2001 (EU internals) are subject to freezing.

(b) For UNSCR 1267/1989 and 1988, the freezing obligation extends to all funds/other assets that belong to, are owned, held or controlled by a designated person/entity. The obligations to freeze the funds or assets of persons and entities to be frozen when acting on behalf of, or at the direction of, designated persons or entities is met by the requirement to freeze funds or assets “controlled by” a designated entity, which extends to persons acting on their behalf in relation to those funds (EU Council Regulation 881/2002 article 2 (1)). For UNSCR 1373, the freezing obligation in EU regulation 2580/2001 (art.1(a) and art.2(1)(a)) applies to assets belonging to, owned or held by the designated individual or entity. It does not apply directly to funds or assets controlled by, or indirectly owned by, or derived from assets owned by, or owned by a person acting at the direction of a designated person or entity. EU regulation 2580/2001 includes provisions empowering the Council to designate any legal person or entity controlled by a designated individual or entity, or a natural person acting on behalf of a designated entity (Art.2(3) (iii) and (iv)) and largely addresses this gap. However, it remains unclear whether this extends to jointly owned funds. While Best practices for the effective implementation of restrictive measures adopted by the Council of the EU (paragraphs 35-36) provide that in practice these funds and economic resources jointly owned are covered in their entirety and thus subject to asset freeze, it is not strictly enforceable. However, this gap is addressed in Finland by Section 11, Chapter 4 of the Enforcement Code which provides that the assets in joint possession may be attached and allows the Enforcement authority to freeze also jointly owned assets.

(c) EU nationals and legal persons incorporated or constituted under the laws of EU Member States are prohibited from making funds or other economic resources available to designated persons and entities (EC Regulations 881/2002 art.2(2), 753/2011 art.3(2), 2580/2001 art 2(1)(b)). Regulations apply to any natural or legal person, entity, body or group in respect of any business done in whole or in part within the Union. The same prohibition is included in the Freezing Act (Section 7).

(d) EU legal acts are published in the Official Journal of the EU and information on the designations is included in the Financial Sanctions Database maintained by the European Commission. National freezing decisions are published in the Official Gazette (EC Regulation 881/2002, Art.13; 753/2011, Art. 15; 2580/2011, Art.11; Freezing Act, Section 4) and NBI maintains a publicly available updated list of such decisions (Freezing Act, Section 8). The MFA provides guidance to FIs and DNFBPs on its webpage information concerning the EU restrictive measures in force (including those implementing UNSCRs), and releases a topical newsletter concerning latest amendments and revisions within the different regimes of restrictive measures. The sanctions newsletter is a regular update of the MFA on new amendments and regulations related to EU sanctions and their application.

(e) Natural and legal persons (including FIs and DNFBPs) are required to immediately provide any information about accounts and amounts frozen (articles 5.1 of EU regulation/881/2002, 4 of EU regulation 2580/2001, 8 of EU Regulation 753/2001, Freezing Act Section 14(3)). This includes attempted transactions as the

scope of the obligation provided by Freezing Act provision encompasses “any information about the funds”.

(f) EU Regulations protect third parties acting in good faith (Regulations 881/2002 art.6; 753/2011 art.7; Freezing Act, Section 15).

Criterion 6.6 –

(a) *At EU level*, there are procedures to seek de-listing through EU Regulations (EC Regulation 753/2011, Art. 11(4) for designations under UNSCR 1988 and EC Regulation 881/2002, art. 7a and 7b1 for UNSCR 1267/1989). *At the national level* however, no publicly known procedures exist with regard to delisting procedures, although the MFA being the competent national authority for the duties imposed by the UNSCRs (Sanctions Act, section 2b (4)) would be the authority to submit the requests to the Committees.

(b) At EU level, for 1373 designations, the EU has de-listing procedures under Regulation 2580/2001. De-listing is immediately effective and may occur ad hoc or after mandatory 6-monthly reviews. *At national level*, the NBI shall assess every six months whether the grounds for freezing the funds continue to exist, and shall without delay reassess the freezing of the funds under circumstances listed in Freezing Act (Sections 11 and 12).

(c) *At the EU level*, a listed individual or entity can write to the EU Council to have the designation reviewed or can challenge the relevant Council Regulation, a Commission Implementing Regulation, or a Council Implementing Regulation in Court, per Treaty on the Functioning of the European Union (TFEU) (article 263 (4)). Article 275 also allows legal challenges of a relevant CFSP Decision. *At the national level*, the freezing decision can be subject to an administrative review (Freezing Act, Section 17). A decision made on a request for a review may be appealed to the Administrative Court of Helsinki, within 30 days after the decision.

(d) & (e) For 1267/1989 and 1988, designated persons/entities are informed of the listing, its reasons and legal consequences, their rights of due process and the availability of de-listing procedures including the UN Office of the Ombudsperson (UNSCR 1267/1989 designations) or the UN Focal Point mechanism (UNSCR 1988 designations). There are EU procedures that provide for de-listing names, unfreezing funds and reviews of designation decisions by the Council of the EU (EC Regulation 753/2011, art.11; EC Regulation 881/2002, art.7a and 7e).

(f) *At EU level*, upon verification that the person/entity involved is not designated, the funds/assets must be unfrozen (EU Regulations 881/2002, 753/2011 and 2580/2001). The EU Best Practices on the implementation of restrictive measures provide guidance on the procedure for cases of mistaken identity (see paras 8-17). *At national level*, if insufficient identifiers make it impossible to verify that the detected party is the party whose assets have been frozen, the person or entity shall inform the Enforcement Authority and act according to its instructions (see FIN-FSA standard 2.4., para 129). These procedures are published on the public website of the MFA.

(g) *At EU level*, legal acts on delisting are published in the Official Journal of the EU and information on the de-listings is included in the Financial Sanctions Database maintained by the European Commission (EC Regulation 881/2002, Art.13;

753/2011, Art. 15; 2580/2011, Art.11). The MFA provides on its webpage information concerning the EU restrictive measures (including those implementing UNSCRs) in force, and releases a topical newsletter concerning latest amendments and revisions within the different regimes of restrictive measures.

Criterion 6.7 – *At EU level*, there are mechanisms for authorizing access to frozen funds or other assets which have been determined to be necessary for basic expenses, the payment of certain types of expenses, or for extraordinary expenses (articles 2a of EU Regulation 881/2002, EU Regulation 753/2011, and 5–6 of EU Regulation 2580/2001). *At national level*, the bailiff enforcing the asset freeze shall ensure that necessary funds to cover basic expenses are given access to as provided for in Enforcement Code (Chapter 4, Section 19). Freezing act provides for similar exemption with regard to funds necessary for basic expenses as determined on a case-by-case basis by the NBI and enforcement authority (Freezing Act, Section 5).

Weighting and conclusion: Finland has minor shortcomings, the main one being that the national mechanism for the implementation of UNSCR 1267/1989 and 1988 needs to be clarified.

Recommendation 6 is rated largely compliant.

Recommendation 7 – Targeted Financial Sanctions related to Proliferation

These obligations were added during the revision of the FATF Recommendations in 2012 and were thus not considered in the framework of the 3rd Mutual Evaluation of Finland.

Criterion 7.1 – *At the EU level*, UNSCR 1718 and successor Resolutions on the Democratic People’s Republic of Korea (DPRK) is transposed into the EU legal framework (Council Regulation 329/2007, Council Decision (CD) 2013/183/CFSP, and CD 2010/413 the current legislative framework is based on Council Decision (CFSP) 2016/849 and Regulation (EU) 2017/1509)). UNSCR 2231 on Iran is transposed into the EU Legal framework through EC Regulation 267/2012 as amended by EC Regulations 2015/1861 and 1862. EU regulations are directly applicable in Finland, as explained under c.6.4. In addition, Finland has legal provisions that would enable it to implement without delay UNSCR obligations directly by decree, without relying on the EU implementation process (Act on the fulfilment of certain obligations of Finland as a Member of the United Nations and of the European Union, “Sanctions Act”).

Criterion 7.2 –

(a) *At the EU level*, the EU Regulations require all natural and legal persons within or associated with the EU to freeze the funds/other assets of designated persons/entities. This obligation is triggered as soon as the Regulation is approved and the designation published in the Official Journal of the European Union (OJEU) (EU Regulation 267/2012, Art. 49; Regulation 2017/1509, Art. 1). However, delays in transposing the UN designations into EU law and the possible difficulties in relying on the criminal justice framework in the interim mean that freezing may not happen without delay for entities which are not already designated by the EU, and raises the question of whether the freezing action, in practice, takes place without prior notice to the designated person/entity.

At the national level, all natural and legal persons are required to freeze funds directly by virtue of EU regulations. A bailiff is in charge of freezing other assets, upon application of the MFA (Sanctions Act, Section 2b(1)).

(b) The freezing obligation under the EU framework extends to all types of funds.

(c) EU nationals and persons within the EU are prohibited from making funds and other assets available to designated persons and entities unless otherwise authorised or notified in compliance with the relevant UNSCRs (articles 6(4) of EU Regulation 329/2007 and 23(3) of EU Regulation 267/2012).

(d) EU legal acts are published in the Official Journal of the EU and information on the designations is included in the Financial Sanctions Database maintained by the European External Action Service. The MFA provides guidance to FIs and DNFBPs on its webpage information concerning the EU restrictive measures in force (including those implementing UNSCRs), and releases a topical newsletter concerning latest amendments and revisions within the different regimes of restrictive measures. The sanctions newsletter is a regular update of the MFA on new amendments and regulations related to EU sanctions and their application. Guidance has been issued by FIN-FSA.

(e) Natural and legal persons (including FIs/DNFBPs) are required to provide immediately any information about accounts and amounts frozen to the enforcement authority, i.e. the bailiff in Finland (articles 10.1 of EU Regulation 329/2007 and 40.1.a of EU Regulation 267/2012). This includes attempted transactions as the scope of the obligation provided by Freezing Act provision encompasses “any “information about the funds”.

(f) EU Regulations protect third parties acting in good faith (Council Regulation (EU) 2017/1509, art.50; Council Regulation (EU) No 267/2012, art.42).

Criterion 7.3 – EU Member States have to take all measures necessary to ensure that the EU regulations are implemented, and have effective, proportionate and dissuasive penalties available for failing to comply with these requirements (EC Regulation 267/2012, art. 47; EC Regulation 329/2007, art. 14). Finland’s AML/CFT supervisors do not have a statutory duty to carry out the supervision of the implementation of the targeted financial sanctions obligations and therefore do not have a power to impose administrative sanctions (see c. 27.1 and 28.2). However, should FIN-FSA suspect that a financial institution has neglected such obligations and a criminal offence (*Regulation offence*) has been committed, it is under legal obligation to refer the matter to the Police for pre-trial investigation (FIN-FSA Act, Section 3 (c)).

The Sanctions Act together with the Criminal Code provide for the penalties and forfeitures to be imposed for violations of EU Council Regulations for both FIs and DNFBPs (*Regulation offence* punishable by a fine or imprisonment for at most 2 years – Chapter 46, Section 1). The supervisory role of RSAA over all DNFBP in this regard is muted, as it appears to have no powers to take administrative action for violations of such EU Council Regulations.

Criterion 7.4 – (*Mostly Met*)

(a) The EU Regulations contain procedures for submitting de-listing requests to the UN Security Council for designated persons or entities that, in the view of the EU, no

longer meet the criteria for designation. The EU Council of Ministers communicates its designation decisions and the grounds for listing, to designated persons/entities, which have the right to comment on them, and to request a review of the decision by the Council (Treaty on the Functioning of the European Union (TFEU), in the fourth paragraph of art. 263 & 275). Such a request can be made regardless of whether a de-listing request is made at the UN level (for example, through the Focal Point mechanism). Where the UN de-lists a person/entity, the EU amends the relevant EU Regulations accordingly.

(b) *At EU level*, the EU Best Practices on the implementation of restrictive measures provide guidance on the procedure on the cases of mistaken identity (see paras 8-17). *At national level*, if insufficient identifiers make it impossible to verify that the detected party is the listed party, the person or entity shall inform the Enforcement Authority and act according to its instructions (see FIN-FSA standard 2.4., para 129). These procedures are published on the public website of the MFA.

(c) There are specific provisions for authorising access to funds or other assets, where the competent authorities of Member States have determined that the exemption conditions set out in resolutions 1718 and 2231 are met, and in accordance with the procedures set out in those resolutions (EU Regulation 329/2007 articles 7 and 8, and EU Regulation 267/2012 articles 24, 26, and 27).

(d) *At EU level*, legal acts on de-listings are published in the Official Journal of the EU and information on the de-listings is included in the Financial Sanctions Database maintained by the European Commission (EC Regulation 881/2002, Art.13; 753/2011, Art. 15; 2580/2011, Art.11). The MFA provides on its webpage information concerning the EU restrictive measures (including those implementing UNSCRs) in force, and releases a topical newsletter concerning latest amendments and revisions within the different regimes of restrictive measures.

Criterion 7.5 –

(a) The EU Regulations permit the payment to the frozen accounts of interests or other sums due on those accounts or payments due under contracts, agreements or obligations that arose prior to the date on which those accounts became subject to the provisions of this resolution, provided that these amounts are also subject to freezing measures (Regulation 329/2007, Art. 9 and Regulation 267/2012, Art. 29).

(b) Provisions in the EU Regulations also authorise the payment of sums due under a contract entered into prior to the designation of such person or entity, provided that this payment does not contribute to an activity prohibited by the regulation, and after prior notice is given to the UN Sanctions Committee (Regulation 267/2012, Art. 24 and 25).

Weighting and conclusion: Finland has minor shortcomings; in particular, there are still some delays in transposing the UN designations into EU law, which raises the question of whether the freezing action takes place without prior notice to the designated person/entity.

Recommendation 7 is rated largely compliant.

Recommendation 8 – Non-Profit Organisations (NPOs)

In its 2007 MER, Finland was rated partially compliant for these requirements. Main shortcomings were that there has been no review of the NPO sector and identification of vulnerabilities; and information was only obtained on those NPOs that are registered and an unknown number of NPO were not registered with authorities. In the 9th FUR of 2013, Finland was still rated partially compliant.

Criterion 8.1 –

(a) Finland has identified a subset of NPOs at risk of TF abuse, but its analysis is not updated, since no comprehensive national review of NPOs has been carried out. However, as part of the 2015 NRA (see c. 1.1 and 3), competent authorities (including supervisory authorities and LEAs) were asked to assess the risks and growth potential of various activities as a means of financing terrorism, including NPOs. The 2014 National counter terrorism strategy, action 12 also dealt with NPOs. A report on "The Financing of Terrorism and Non-Profit Organisations" (which involved the National Police Board, the National Bureau of Investigation, the Finnish Security Intelligence Service and prosecutors) was completed in 2009. On this basis, Finland has identified a serious risk and significant growth potential in the abuse of immigrant-based associations. NPOs receiving state subsidies, collecting money and humanitarian aid to crisis areas were also identified as potentially at risk. The FIU has confirmed in 2018 these findings on the basis of an analysis of STRs related to NPOs received between 2016 and 2018 which has not been disseminated as confidential information.

(b) Finland points out to the possible types of NPOs at specific risk of abuse for TF (see a), and has begun to identify through FIU work, including strategic analysis, the specific nature of threat(s) and how terrorist actors could abuse those NPOs (including in the counter terrorism strategy, actions 12 and 29).

(c) Upon the AML/CFT Act (Chapter 2, Section 7), the obligation to identify beneficial owners and to keep the information up-to-date has been extended to associations and religious communities. Members of the boards of directors are "deemed to be" the beneficial owners according to these provisions. This law targets partly the subset of NPOs at risk and the measures introduced remain limited.

(d) The 2009 report on "The Financing of Terrorism and Non-Profit Organisations" has not been updated. The 2015 NRA, which reviewed NPOs to some extent, has not yet been updated. The National counter terrorism strategy, including action 12 which targets TF, is periodically updated (2014, 2016), but this does not specifically cover the NPO sector.

Criterion 8.2 –

(a) Finland has policies to provide transparency in the setting up and activities of some NPOs, to promote accountability, integrity and public confidence in the administration and management of the sector. Associations under an obligation to register include religious communities (Associations Act, Section 48; Freedom of Religion Act). Foundations are also registered (Foundations Act, Chapter 13, Section 2). The basic information on associations, religious communities and foundations, including "deemed" beneficial owners, are entered in public registers (Associations Act (503/1989), Sections 48 and 52; Freedom of Religion Act (453/2003), Sections

18 and 20; Foundations Act (487/2015), Chapter 13, Sections 1, 4 and 6). All those registers are maintained by the Finnish Patent and Registration Office (PRH) (Finnish Patent and Registration Office Act; Associations Act, Section 47; Freedom of Religion Act, Section 15; Foundations Act, Chapter 13, Section 1). The PRH has wide powers to monitor foundations, e.g. request and review information/documents (Foundations Act, Chapter 14). An audit shall be carried out in all foundations (Foundations Act, Chapter 4, Section 1). The registered associations, religious communities and foundations are subject to accounting obligations that are the same as the ones applicable to limited liability companies regarding keeping accounting records (Accounting Act, Chapter 1 section 1(1)).

As a rule, registered associations, religious communities and foundations may be given the right by the local police or the National Police Board, upon application, to organise money collections (Money Collections Act, Section 7). There are also some associations which are not obliged to register and have the capacity of raising and disbursing money, where they have a non-profit purpose and their status is based on law (e.g. Red Cross, student union of a university, interdisciplinary associations of students) or they have a non-profit purpose and their activities are temporary (e.g. support associations for candidates in general elections and support groups for the support of individuals or families that have been victims of accidents) (Money Collections Act, Section 7(2)). However, those situations are limited under the Money Collections Act. Those non-registered associations are not legal persons, they have no assets of their own and cannot assume legal liability for their actions. However, non-registered associations are still comparable with registered associations in respect of the obligation to keep accounting records. The persons acting on behalf of a non-registered association (or persons who have made decisions on its behalf) are personally and jointly liable for its actions (Associations Act, Chapter 10, Section 50). If such persons carried out business or professional activities for themselves, they would be subject to accounting obligations for natural persons (Accounting Act, Chapter 1, Section 1 (a)).

For registered associations, an auditor is appointed, provided the thresholds⁹⁵ of the Auditing Act are met (Chapter 2, Section 2). The scope of audits covers the governance of the audited association for the financial year, in addition to accounting records and the financial statements (Auditing Act, Chapter 3, Section 1). Associations who do not have auditors have an operations inspector, who will review their finance (Associations Act, Section 38 a).

(b) Limited outreach activities have been conducted to raise awareness of the TF risks relating to the NPO sector and they cannot be considered as educational programmes. The National Police Board has published a link to the 2009 report (see c. 8.1 d)), as well as links to the 2013 FATF Best Practices on Combating the abuse of NPOs and to the 2014 FATF Report on the Risk of Terrorist Abuse in Non-Profit Organisations on its website. It has also published guidelines on money collection authorisations and conditions. The National Counter Terrorism Strategy includes an

⁹⁵ “There is no obligation to appoint an auditor for a corporation where no more than one of the following conditions were met in both the last completed financial year and the financial year immediately preceding it: 1) the balance sheet total exceeds EUR 100,000; 2) the net sales or comparable revenue exceeds EUR 200,000; or 3) the average number of employees exceeds three”.

action (action 9) to increase cooperation between public authorities and the private sector in the prevention of terrorism. Finnish authorities have also organised seminars and meetings with representatives of the NPO sector.

(c) There has been no work with NPOs to develop and refine best practices.

(d) Due to the accounting obligation of associations, operations inspection or auditing and permit requirement for money collections (see c. 8.2a)), in practice money collections by NPOs are mainly organised using regulated channels. As regards permits to collect money, one of the conditions is that the NPO opens a bank account for the money collection (Money Collections Act, section 17). This requirement to use a bank account also applies to money collected in cash. Should associations carry out business activities, and have taxable income, they would be subject to legislation governing the particular field of business and taxation.

Criterion 8.3 – Finland has taken general steps to promote effective supervision or monitoring that help preventing the misuse of money collection for TF. However, it does demonstrate only to a limited extent that risk-based measures apply to NPOs at risk of TF abuse. Measures implemented are not exclusively targeting the subset of NPOs at risk of TF abuse, but cover the activity all NPOs (money collection).

All NPOs are subject to monitoring by the National Police Board regarding money collection, but there is limited information available regarding risk-based actions that would have been taken. The National Police Board formulates annually an inspection plan for money collections, which defines targets and identifies focuses for the inspections. In 2018, the focus includes money collections in which collected funds can be sent abroad and money collections in which the permit receiver collects cash.

The MFA has been given responsibility to monitor the use of state subsidies by NPOs that receive such subsidies under law, and has powers to carry out on-site inspections through its diplomatic representations (*Act on Discretionary Government Transfers*, Sections 15, 16, 17 and 19). However, this does not amount to the conduct of supervisory activities and risk-based actions as these actions are not limited to NPOs receiving state subsidies, collecting money and humanitarian aid for crisis areas or high risk-countries but do apply to all NPOs receiving state funding irrespective of the nature or size of associations which have been identified at risk of TF abuse. Only the subset of NPO receiving state subsidies and having activities in risk areas are subject to additional monitoring by the MFA, which is primarily targeted at protecting the use of public funding, rather than protecting these NPOs against TF abuse. Partial identification of the subset of NPOs at risk of TF abuse (see c.8.1 a)) has an impact on effective supervision or monitoring of these NPOs.

All registered NPOs (see c. 8.2.a) are under an obligation to undergo operations inspection or auditing. All foundations shall undergo auditing and are supervised by the PRH. Auditors as such do not fall within the scope of FATF reporting entities, unless they carry out one of the activities listed in the FATF Glossary. They are obliged entities who have, under the AML/CFT Act, an obligation to carry out their own risk assessments, which should include risk factors linked to their (NPO) customers and report suspicions of TF to the FIU. This does not amount to AML/CFT monitoring or supervision, but is a positive step to review the activities of registered associations and flag any TF suspicion. The PRH is the authority responsible for the

registers of NPOs, but does not have an AML/CFT monitoring or supervisory role vis-à-vis NPOs in this function. As the AML/CFT supervisor of auditors (see R. 20 and 28), the PRH has a reporting obligation of suspicious transactions to the FIU vis-à-vis auditor, but this would not apply directly vis-à-vis NPOs, as customers of auditors.

Criterion 8.4 –

(a) The National Police Board has general competence and responsibility for guidance and supervision in relation to money collection, including by those entities that have been given permit to conduct such activities and those which operate without licence which are part of the subset of NPOs at risk (see c. 8.1 and 2) (Money Collection Act, Section 26). The National Police Board thus provides guidance and interprets the law and may also file criminal complaints to the police in relation to money collection. The general duties of auditors on registered associations include reviewing the accounting records, the financial statements, and the governance of the audited entity (see c. 8.3). Risk-based measures being applied remain however limited, as seen notably in c.8.1 and c.8.3, which has a negative impact on this criterion.

(b) Sanctions are in place for NPOs or persons acting on behalf of these NPOs but those are not fully proportionate and dissuasive (see c.5.7). The Criminal Code provides for a money collection offence and a petty money collection offence, which is the confiscation of the proceeds of those criminal offences (Chapter 10). Other criminal offences committed in the course of activities of NPOs would be punishable under the relevant provisions of the Criminal Code (e.g. accounting offence) or of the Accounting Act. The criminal liability of legal persons applies to money collections offences and TF offences, but some gaps in the applicable regime have been identified (see c. 5.7). Fines are applicable to foundations and associations when they neglect to submit financial records to PRH (Accounting Act, Chapter 8, Section 4; Foundations Act, Chapter 10, Section 2). Sanctions for violations of certain accounting obligations are applicable, including regarding the obligation to maintain accounting reports (Accounting Act, Chapter 8, section 4 (fine); Criminal Code, Chapter 30, sections 9 (accounting offence: fine or imprisonment for at most 2 years), 9(a) (aggravated accounting offence: imprisonment from 4 months to 4 years), and 10 that provide fines and imprisonment (negligent accounting offence: fine or imprisonment for at most 2 years)).

Criterion 8.5 –

(a) There is ad hoc co-operation, coordination and information sharing among appropriate authorities (National Police Board, PRH), but it is not focused on NPOs. In 2010, a broad-based counter-terrorism working group was set up (Decision on setting up the Cooperation Group for the prevention of terrorism, 15.6.2010 SMD no/2010/1050) with representatives from all interested public offices (Immigration services, Minister of the Interior, Police, Intelligence services, etc.). The working group's tasks include coordinating co-operation between authorities for terrorism-related issues, and making use of expert networks of different authorities in combating terrorism. Although the work of this group does not include a specific focus on NPOs, it could constitute a platform for coordination on this.

(b) The investigative expertise and capability to examine those NPOs suspected of either being exploited by, or actively supporting, terrorist activity or terrorist organisations is ensured by the National Bureau of Investigation (see R. 30 and 31).

(c) The Police Act and the Coercive Measures Act ensure full access to information on the administration and management of particular NPOs (including financial and activities information) during the course of an investigation (Police Act, Chapter 4 sections 2 and 3; Coercive Measures Act, Chapter 7 section 1). Both the NPOs and the accountants would be under an obligation by law to provide the requested information to the police, supplemented by coercive means available (see c. 31.1).

(d) The general powers of investigative bodies provide for the relevant procedures to ensure that –under situations described in the criterion – relevant information is shared with competent authorities, in order to take preventive or investigative actions (Police Act, Chapter 4 section 3; Coercive Measures Act, Chapter 7 section 1). Even though it is clear under the Criminal Investigation Act (Chapter 3, Section 11, Period of conduct of the criminal investigation Subsections 1 and 3) that *“the criminal investigation shall be conducted without undue delay”* and that *“when required by the circumstances, the criminal investigation measures may be placed in order of priority”*, there is no reference to the need to act *“promptly”* as regards sharing of information with other competent authorities. In addition, it is unclear through which mechanism the relevant information detained by the FIU on NPOs would circulate to investigative bodies and there is no obligation for the FIU to *“promptly”* share information as the FIU Act provides only that *“the information obtained (by the FIU) may be used and disclosed (...)”* (Section 4, paragraph 4).

Criterion 8.6 – The points of contact and procedures to respond to international requests for information regarding particular NPOs suspected of terrorist financing or involvement in other forms of terrorist support are the same as for any other terrorist or terrorist financing suspicions, particularly the law enforcement channels for exchange of information (see c. 37.2).

Weighting and conclusion: There is a limited identification of the subset of NPOs at risk of TF abuse and of the nature of threats. This has an impact on the scope and implementation of risk-based supervision and monitoring measures.

Recommendation 8 is rated partially compliant.

Recommendation 9 - Financial institution secrecy laws

In its 3rd MER, Finland was rated compliant with these requirements (para.418-427).

Criterion 9.1 – There are a number of provisions in the Finnish legislation that provide for exemptions from the financial institution secrecy laws.

Access to information of competent authorities

A prosecuting and criminal investigation authority for the investigation of a crime, as well as another authority entitled to information held by financial institutions under the law (such as the bailiffs), have the right to access information held by financial institutions (Act on Credit Institutions, Chapter 15, Section 14, subsection 2; Act on the Supervision of Financial and Insurance Conglomerates, section 33 subsection 2; Act on Payment Institutions, section 37, subsection 2; Act on Alternative investment fund managers (AIFMs), Chapter 7, section 11; Act on

Investment Services, Chapter 12, Section 2; Insurance Companies Act Chapter 30, section 3 subsection 8; Act on Foreign Insurance Companies Chapter 11 section 79; Act on the Book-Entry System and Settlement Activities Chapter 8, sections 1-2; Act on Common Funds, Section 133; Enforcement Code, Chapter 3, Sections 64 and 66).

FIN-FSA has the right to obtain access to the documents and other records and information systems to the extent necessary to perform supervisory duties (FIN-FSA Act, Chapter 3, Section 24). The FIU has the right to request any information from financial institutions (FIU Act, Section 4), as well as the Tax authorities (Act on Taxation Procedure, Section 19).

Sharing of information between competent authorities

Tax authorities can share financial information with the FIU and other LEAs (Act on the public disclosure and confidentiality of tax information, Section 18, subsection 6). FIN-FSA has also the right to share information with other authorities domestically, in the EEA and with similar bodies outside the EEA (FIN-FSA Act, section 71, items 12 and 15).

Sharing of information between financial institutions (R. 13, 16 and 17)

Financial institutions have the right to disclose information to a stock exchange, or a body of stock exchanges (Securities Market Act, Chapter 11, Section 29; Act on Trading in Financial Instruments, Chapter 8, section 3; Act on AIFMs, Chapter 7, section 11; Act on Investment Services, Chapter 12, Section 2). Credit institutions and Payment institutions have right to disclose information to an undertaking in the same financial and insurance conglomerate⁹⁶ (Act on Credit Institutions Chapter 15, section 15, Act on Payment Institutions section 38). An account operator, a settlement agent, a nominee, a CCP, a CSD and an entity to which activities have been outsourced, their holding company and a financial institution belonging to their group have the right to disclose certain information to an entity of the same conglomerate (Act on the Book-Entry System and Settlement Activities Chapter 8, sections 1-2). Management companies are entitled to disclose information to an organisation belonging to the same conglomerate for the purpose of the risk management (Act on Common Funds, section 133a). A member or deputy member of a body or a functionary of a stock exchange may disclose information to a person who is employed by or a member of a body of an organisation operating trading in another State corresponding to a stock exchange and subject to supervision by the authorities (Act on Trading in Financial Instruments Chapter 10, section 2). AIFMs and Investment Services providers have the right to share information within a financial group (Act on AIFMs, Chapter 7, section 11; Act on Investment Services, Chapter 12, and Section 2).

A branch of a Foreign Payment Institution in Finland has the right to provide information to the supervision authority corresponding to FIN-FSA of the country that granted authorisation to the foreign payment institution represented by the branch and to the auditor of the foreign payment institution represented by the branch (Act on the Activities of Foreign Payment Institutions in Finland section 11).

⁹⁶ This term also includes “financial group”, “consolidation group”, or “consortium”

All financial institutions have the right to share STR information within a financial or insurance group authorised in Finland, another EEA Member State, or third country that is subject to equivalent obligations (AML/CFT Act, Chapter 4, Section 4). Financial institutions are allowed to disclose information relevant for risk management according to relevant Acts and their Sections mentioned above (e.g. Act on Credit Institutions Chapter 15 Section 15, Act on Investment Services Chapter 12, Section 2, Act on Payment Institutions Section 38, etc.)

Weighting and Conclusion:

Recommendation 9 is rated compliant.

Recommendation 10 – Customer Due Diligence

In its 3rd MER, Finland was rated partially compliant with these requirements (para. 362-392). The main deficiencies related to the absence of requirements to identify the beneficial owners of legal persons, understand the ownership and control structure, conduct ongoing due diligence, and limited enhanced due diligence obligations. Since then, the FATF Recommendations have been strengthened to impose more detailed requirements, particularly regarding the identification of legal persons and legal arrangements.

Criterion 10.1 – Credit institutions and undertakings belonging to the same conglomerate as well as payment institutions are prohibited from keeping anonymous accounts (Act on Credit Institutions, Chapter 15, Section 18, Act on Payment Institutions, Section 39). There is no direct prohibition from keeping anonymous/fictitious names accounts (or similar business relationships) for other types of financial institutions.

Criterion 10.2 – Financial institutions are required to undertake CDD in all circumstances set out in items (a) to (e) (AML/CFT Act, Chapter 3, Section 2).

Criterion 10.3 – Financial institutions are required to identify customers and verify their identities using reliable sources (AML/CFT Act, Chapter 3, Sections 2 and 3).

Criterion 10.4 – Financial institutions are required to verify that any person purporting to act on behalf of the customer is so authorised, and identify and verify the identity of that person (AML/CFT Act, Chapter 3, Section 2, subsection 3).

Criterion 10.5 – Financial institutions are required to identify the beneficial owner and take reasonable measures to verify the identity of the beneficial owner (AML/CFT Act, Chapter 3, Section 6); however, this requirement does not extend to customers which are natural persons.

Criterion 10.6 – Financial institutions are required to understand and obtain information on the purpose and intended nature of the business relationship (AML/CFT Act, Chapter 3, Section 4).

Criterion 10.7 –

(a) Financial institutions are required to conduct ongoing due diligence on the business relationship, including scrutinising transactions to ensure they are consistent with the financial institution’s knowledge of the customer, their business and risk profile, including the source of funds (AML/CFT Act, Chapter 3, Section 4)

(b) Financial institutions are required to ensure that documents, data or information collected under the CDD process are kept up-to-date and relevant (AML/CFT Act, Chapter 3, Section 3).

Criterion 10.8 – For customers that are legal persons or legal arrangements, financial institutions are required to understand the nature of the customer’s business, ownership and control structures (AML/CFT Act, Chapter 3, Section 3). This is also reinforced through beneficial owners (BO) obligation (AML/CFT Act, Chapter 3, Section 6), see c. 10.5.

Criterion 10.9 – For customers that are legal persons or legal arrangements, financial institutions are required to identify the customer and verify its identity through the following information:

(a) Name, legal form and proof of existence (AML/CFT Act, Chapter 3, Section 3, subsection 2, item 3);

(b) The names of the relevant persons having a senior management position (AML/CFT Act, Chapter 3, Section 3, subsection 2, item 4), however there is no requirement concerning powers that bind and regulate legal person/arrangement.

(c) There is no explicit requirement with regard to the address of the registered office or a principal place of business.

Criterion 10.10 – For customers that are legal persons, financial institutions are required to identify and take reasonable measures to verify the identity of beneficial owners which includes all of the elements set out in items (a) to (c) (AML/CFT Act, Chapter 3, Section 3, and Chapter 1, Sections 5 and 7).

Criterion 10.11 – For customers that are foreign trusts or similar legal arrangements, financial institutions are required to identify and take reasonable measures to verify the identity of beneficial owners which includes all of the elements set out in items (a) to (b) (AML/CFT Act, Chapter 3, Section 3, and Chapter 1, Sections 6).

Criterion 10.12 – Financial institutions are required to conduct the CDD measures on the beneficiary of life insurance and other investment related insurance policies, as set out in the items (a) to (c) (AML/CFT Act, Chapter 3, Section 5).

Criterion 10.13 – Financial institutions are required to include the beneficiary of a life insurance policy as a relevant risk factor in determining whether enhanced CDD measures are applicable, and are required to take enhanced measures at the time of payout (AML/CFT Act, Chapter 3, Section 5, subsection 5).

Criterion 10.14 – Financial institutions are not allowed to establish relationships or conduct transactions prior to conducting CDD (AML/CFT Act, Chapter 3, Section 1).

Criterion 10.15 – (N/A) Not applicable (see c.10.14).

Criterion 10.16 – Financial institutions are not allowed to maintain the existing relationship if they have not carried out the CDD, which essentially means they have to apply it to the existing customers (AML/CFT Act, Chapter 3, Section 1).

Criterion 10.17 – Financial institutions are required to perform enhanced due diligence where the ML/TF risks are higher (AML/CFT Act, Chapter 3, Section 10).

Criterion 10.18 – Financial institutions are allowed to apply simplified due diligence measures (SDD) when ML/TF risks are “negligible”, on the basis of their risk assessment (AML/CFT Act, Chapter 3, section 8, subsection 1). A government decree may define factors indicating situations when the risks can be viewed as “negligible” (Chapter 3, section 8, subsection 2). Government decrees were still under consideration as of the end of the on-site visit. Customers must be identified in all cases of suspicious transactions (AML/CFT Act Chapter 3, section 2, subsection 3), but there is no exemption from SDD measures when there is a suspicion of ML/TF.

Criterion 10.19 – Where a financial institution is unable to comply with relevant CDD measures:

(a) It may not establish business relationships, conclude a transaction or maintain a business relationship (AML/CFT Act, Chapter 3, Section 1).

(b) There is no explicit requirement to consider making a suspicious transaction report. However, there is a general obligation for financial institutions to report, without delay, any suspicious transaction or suspected terrorist financing to the FIU (AML/CFT Act, Chapter 4, Section 1).

Criterion 10.20 – Financial institutions are permitted not to pursue CDD process when they believe that performing the CDD process will tip-off the customer (AML/CFT Act, Chapter 3, Section 1). Financial institutions are required to report “any suspicious transaction or suspected terrorist financing” to the FIU without delay (AML/CFT Act, Chapter 4, Section 1).

Weighting and Conclusion: Not all types of financial institutions are prohibited from keeping anonymous accounts (or similar business relationships). There is no obligation not to apply SDD measures when there is a suspicion of ML/TF. There are also some minor deficiencies with regard to the scope of information that financial institutions are required to collect from their customers.

Recommendation 10 is rated largely compliant.

Recommendation 11 – Record keeping

In its 3rd MER, Finland was rated compliant with these requirements (para. 428-433).

Criterion 11.1 – There is a general requirement that all transactions of legal persons, including financial institutions, are required to be recorded and kept for at least 10 years from the end of the financial year (Accounting Act, Chapter 2, Section 10). Furthermore, funds that are managed on behalf of clients must be disclosed as a separate item in the balance sheet (Accounting Decree 1337/1997, Chapter 1, Section 6, subsection 5). The requirements extend to all ledgers and sub-ledgers which contain records of customer funds and single transactions.

Criterion 11.2 – Financial institutions are required to keep all records obtained through CDD, account files and results of analysis for five years from end of the permanent customer relationship. In the case of occasional transactions, CDD information is required to be retained for a period of five years from conclusion of the transaction (AML/CFT Act, Chapter 3, Section 3). According to the Explanatory

memorandum of the AML/CFT Act (see Chapter 1), such requirements also include business correspondence.

Criterion 11.3 – The keeping of accounting records shall be arranged so that the connection between transactions through any sub-ledgers with the general ledger and from it to the financial statements is verifiable without difficulty in both directions (Accounting Act, Chapter 2, Section 6).

Criterion 11.4 – Financial institutions are required to supply the supervisory authorities with the information and reports requested by them without undue delay and free of charge (AML/CFT Act, Chapter 7, section 2). Financial institutions are also obliged to provide, free of charge, the FIU with all data, information and documents necessary to investigate reported suspicions. Financial institutions shall respond to the FIU requests for information within the reasonable period of time determined by the FIU (AML/CFT Act, chapter 4, section 1). Competent authorities conducting investigations have powers to use compulsory measures for the production of records held by FIs, DNFBPs and other natural or legal persons (Police Act, Chapter 4, sections 2-4; Criminal Investigation Act and Coercive Measures Act, Processing of Personal Data by the Customs, section 13).

Weighting and Conclusion:

Recommendation 11 is rated compliant.

Recommendation 12 – Politically Exposed Persons (PEPs)

In its 3rd MER, Finland was rated non-compliant with these requirements (para. 393-394). In 2012, FATF introduced new requirements for domestic PEPs and PEPs from international organisations.

Criterion 12.1 – In relation to foreign PEPs, financial institutions are required to:

(a) put in place risk management systems to determine whether a customer is a PEP (AML/CFT Act, Chapter 3, Section 13, subsection 1).

(b)-(d) obtain senior management approval before establishing (or continuing for existing customers), take measures to establish the source of wealth and funds, and conduct enhanced ongoing monitoring (AML/CFT Act, Chapter 3, Sections 1 and 13).

There is no requirement to determine whether a beneficial owner of a customer is a PEP.

Criterion 12.2 – The legal provisions concerning PEPs apply equally to domestic and foreign PEPs. Therefore, all elements of this criterion are observed (AML/CFT Act, Chapter 3, Section 13).

Criterion 12.3 – All requirements with regard to PEPs are equally applicable to their family members and associates (AML/CFT Act, Chapter 3, Section 13).

Criterion 12.4 – In relation to life insurance policies, financial institutions are required to take measures to determine whether the beneficiaries are PEPs, at the latest at the time of the payout. Financial institutions are also required to inform senior management before the payout of the policy proceeds, and to conduct enhanced due diligence (AML/CFT Act, Chapter 3, Section 5, subsection 5). There is

requirement to consider making an STR in case of higher risks (AML/CFT Act, Chapter 3, Section 5, subsection 5).

Weighting and Conclusion: There is no requirement to determine whether a beneficial owner of a customer is a PEP.

Recommendation 12 is rated largely compliant.

Recommendation 13 – Correspondent Banking

In its 3rd MER, Finland was rated non-compliant with these requirements (para. 395-397). The new FATF Recommendation adds a specific requirement concerning the prohibition of correspondent relationships with shell banks.

Criterion 13.1 – All elements of this criterion (a) to (d) are covered by AML/CFT Act, Chapter 3, Section 12. However, these requirements apply only to non-EEA states.

Criterion 13.2 – All elements of this criterion (a) to (b) with regard to “payable-through accounts” are set out in AML/CFT Act, Chapter 3, Section 12, subsection 5. However, these requirements apply only to non-EEA states.

Criterion 13.3 – Financial institutions are prohibited from entering into relationships with shell banks (AML/CFT Act, Chapter 3, Section 12, subsection 3).

Weighting and Conclusion: Correspondent banking requirements do not apply to EEA countries.

Recommendation 13 is rated partially compliant.

Recommendation 14 - Money or Value Transfer Services (MVTs)

In its 3rd MER, Finland was rated partially compliant with these requirements (para. 602-607). The main deficiencies were: remittance services were not required to develop internal controls; there was no monitoring or supervision of the sector; and remittances services were subject only to criminal sanctions. There were also concerns with regard to the effectiveness of the STR reporting obligation which is not assessed as part of technical compliance under the 2013 Methodology. FATF introduced new requirements concerning the identification of MVTs providers who are not authorised or registered.

- Money and value transfer services can be carried out by: Credit Institutions according to Act on Credit Institutions, Chapter 5, section 1
- Payment institutions and payment service providers according to Act on Payment institutions, Chapter 1, section 1

Criterion 14.1 – There are licensing requirements both for credit institutions (Act on Credit Institutions, Chapter 2, section 1) and payment institutions (Act on Payment institutions, Chapter 2, section 6). If the average of the preceding 12 months' total amount of the payment transactions executed does not exceed a) EUR 3 million per month for a legal person; or b) EUR 50 000 per month for a natural person, then the payment provider needs only to be registered (Act on Payment institutions, Chapter 2, section 7).

Criterion 14.2 – Finland takes action with a view to identifying service providers without license or registration – FIN-FSA maintains a system for receiving reports of suspected infringements of financial market provisions (whistleblowing system) (Act on Financial Supervisory Authority, Chapter 8, Section 71a).

There are sanctions for unauthorised provision of services:

- A fine or one year of imprisonment under the Act on Credit institutions (Act on Credit Institutions, Chapter 21, section 2)
- A fine or 6 months of imprisonment under the Act on Payment institutions (Act on Payment institutions, Chapter 8, section 49)

The sanctions appear to be proportionate and dissuasive.

Criterion 14.3 – MVTS are subject to monitoring for AML/CFT compliance (AML/CFT Act, Chapter 7, Section 1).

Criterion 14.4 – Credit institutions and payment service providers are required to notify their agents to FIN-FSA, which apparently includes agents in all countries where the MVTS provider operates (Act on Credit institutions, Chapter 5, section 10; Act on Payment institutions, Chapter 4, section 24).

Criterion 14.5 – Credit institutions are only allowed to use agents if this does not impair the risk management or internal control of the credit institution (which includes AML/CFT programmes), and they are required to continuously obtain information from the agents in that regard (which ensures monitoring of their compliance) (Act on Credit institutions, Chapter 5, sections 10 and 11).

A comparable requirement exists for Payment institutions (Act on Payment institutions, Chapter 4, section 23).

Weighting and Conclusion:

Recommendation 14 is rated compliant.

Recommendation 15 - New Technologies

In its 3rd MER, Finland was rated partially compliant with these requirements (para. 398-403). The main deficiencies related to the absence of requirements for obliged parties to have measures in place for prevention of the misuse of technological developments in ML or TF, and limited provisions with respect to non-face-to-face business relationships and transactions. The new R. 15 focuses on assessing risks related to the use of new technologies, in general, and no longer specifically targets distance contracts.

Criterion 15.1 – AML/CFT Act, Chapter 2, sections 2 and 3 require supervisors and financial institutions to update regularly risk assessments and also update in the event of material change in activities. More specifically, in assessing ML/TF risks financial institutions shall take into account risks relating to delivery channels and technologies (AML/CFT Act, Chapter 3, section 1, subsection 2). However, this does not seem to extend to situations when a financial institution is considering the development of the new product or service *before* the offering to customers.

Finland has identified several ML/TF risks related to new products, business practices and technologies, such as mobile payments, remote authentication, real-time online payments, and use of virtual currencies (NRA 2015, see c. 1. 1 and 3), but has not assessed those risks.

Criterion 15.2 –

(a) Financial institutions (with the exception of consumer credit providers, currency exchange providers, and other financial service providers supervised by RSAA, see R. 26 for further details) are required to assess the risks of a new product and service (AML/CFT Act, Chapter 3, Section 1 and Chapter 2, Section 3). However, only financial institutions supervised by the FIN-FSA are required to do it prior to their introduction (FIN-FSA Regulations and guidelines 8/2014, Section 4.3, para. 11).

(b) Most financial institutions (with the exception of consumer credit providers, currency exchange providers, and other financial service providers supervised by RSAA) should also confirm the necessary risk mitigation methods and other necessary corrective measures, as well as decide on an acceptable risk-taking level and set limits and other restrictions for the risks (FIN-FSA Regulations and guidelines 8/2014, Section 4.3, para. 12-13).

Weighting and Conclusion: There are some deficiencies with the scope of the risk-based requirements related to the use of new products, business practices and technologies.

Recommendation 15 is rated largely compliant.

Recommendation 16 – Wire Transfers

In its 3rd MER, Finland was rated partially compliant with these requirements (para. 434-444). The main deficiencies related to the provisions relating to originator information for wire transfers within the EU, absence of obligation to maintain address details, and absence of penalties applicable to infringements of the wire transfer requirements for the money remittance sector. Significant changes were made to the requirements in this area during the revision of the FATF Standards. Furthermore, following the third round evaluation, Regulation (EC) No. 1781/2006 on Information on the payer accompanying transfers of funds, then replaced by Regulation 2015/847, which laid down obligations for FIs when handling wire transfers. This EU Regulation is applicable in Finland and is assessed below.

Criterion 16.1 – All wire transfers are required to be accompanied by information with regard to the payer (originator) and the payee (beneficiary) as set out in the criterion. Originator information has to be verified (Regulation (EU) 2015/847, Article 4).

Criterion 16.2 – Requirements concerning batch transfers, where the payment service providers of the beneficiary are established outside the EU, are covered by Article 6(1) of the Regulation (EU) 2015/847.

Criterion 16.3 – According to Article 6(2) of the Regulation (EU) 2015/847, there is a *de minimis* threshold of EUR 1000 for cross-border wire transfers, below which all of the requirements of the criterion apply.

Criterion 16.4 – Financial institutions are required to verify the information mentioned in criterion 16.3 for accuracy when there is a ML/TF suspicion (Regulation (EU) 2015/847, Article 6(2)).

Criteria 16.5-16.6 – Domestic wire transfers are required to be accompanied by at least payment account number or unique transaction identifier for both originator and beneficiary. The originator financial institution is required to provide all wire transfer information to the beneficiary institution within 3 days of receiving

corresponding request (Regulation (EU) 2015/847, Article 5). Law enforcement authorities are able to compel production of such information (see also c. 9.1 and c.31.1).

Criterion 16.7 – The ordering financial institution is required to maintain all originator and beneficiary information collected for a period of five years (Regulation (EU) 2015/847, Article 16).

Criterion 16.8 – The ordering financial institution is not allowed to execute the wire transfer if it does not comply with the requirements specified above (Regulation (EU) 2015/847, Article 4(6)).

Criterion 16.9 – Intermediary institutions shall ensure that all the information received on the originator and the beneficiary that accompanies a transfer of funds is retained with the transfer (Regulation (EU) 2015/847, Article 10).

Criterion 16.10 – This criterion is not applicable, because there are no limitations in the domestic system. Finland's payments are processed via European payment systems e.g. Target 2 and EBA Clearing, which require full payment details and there are no technical limitations preventing or restricting the data that can be entered into that system. No separate domestic payment systems exist in Finland at this time.

Criteria 16.11-16.12 – Intermediary financial institutions are required to take measures to identify wire transfers missing required information and to have risk-based policies and procedures for determining when to execute, reject, or suspend such wire transfers and the appropriate follow-up action (Regulation (EU) 2015/847, Article 12).

Criterion 16.13 – Beneficiary financial institutions are required to take reasonable measures, including where appropriate post-event monitoring or real-time monitoring where feasible, to identify cross-border wire transfers that lack required information (Regulation (EU) 2015/847, Article 7(1) and 7(2)).

Criterion 16.14 – For cross-border wire transfers of EUR 1000 or more, a beneficiary financial institution is required to verify the identity of the beneficiary (Regulation (EU) 2015/847, Article 7(3)). Record keeping requirements as set out in R.11 apply as well.

Criterion 16.15 – Beneficiary financial institutions shall implement effective risk-based procedures for determining whether to execute, reject or suspend a transfer of funds lacking the required complete information and for taking the appropriate follow-up action (Regulation (EU) 2015/847, Article 8).

Criterion 16.16 – Regulation (EU) 2015/847 applies to all categories of payment service providers, including MVTS (Regulation (EU) 2015/847, Article 3, point 5).

Criterion 16.17 – The payment service provider of the payee shall take into account missing or incomplete information on the payer or the payee as a factor when assessing whether a transfer of funds, or any related transaction, is suspicious and whether it is to be reported to the FIU (Regulation (EU) 2015/847, Article 9).

Criterion 16.18 – FIs are subject to the requirements of the EU regulations which give effect to UNSCR 1267, 1373 and successor resolutions.

Weighting and Conclusion:

Recommendation 16 is rated compliant.

Recommendation 17 - Reliance on Third Parties

In its 3rd MER, Finland was rated non-compliant with these requirements (para. 411-416). The FATF's new requirements emphasise the country risk related to the third party required to perform due diligence on the customer.

Criterion 17.1 – Financial institutions are allowed to rely on 3rd parties which are financial institutions registered in Finland or abroad, with the exception of (AML/CFT Act, Chapter 3, Section 7):

- l) 1) a payment institution which provides the money remittance referred to in the Act on Payment Institutions as a primary payment service;
- m) 2) a natural or legal person referred to in section 7 or 7a of the Act on Payment Institutions; or
- n) 3) a party engaging in currency exchange.

(a)-(b) Before carrying out transactions, financial institutions should obtain customer identification information from the 3rd party, and ensure that all CDD data are available to them on request (AML/CFT Act, Chapter 3, Section 7). The AML/CFT Act does not specifically state that such data and documentation should be made available without delay.

(c) Financial institutions may rely on 3rd parties only if they are subject to CDD and record keeping requirements equivalent to the Finnish ones (in case of EEA-Member States), or if they are established in a non-EEA Member State whose AML/CFT system does not pose threat to the EU Internal Market (AML/CFT Act, Chapter 3, Section 7). The requirement of “not posing threat to the internal market” is not specific enough to meet the requirements of 17.1.(c), as it does not refer to specific obligations regarding being regulated, and supervised or monitored for compliance with CDD and record keeping requirements.

Criterion 17.2 – When determining where the 3rd party can be based, the level of country risk is only considered if the country is not an EEA-Member (AML/CFT Act, Chapter 3, Section 7), which is narrower than the requirement of this sub-criterion.

Criterion 17.3 –

In case of financial groups, the supervisory authority may consider the conditions relating to the 3rd party to be fulfilled if:

- the group or consortium complies with internal procedures common to the group or consortium and equivalent to the provisions of the Finnish legislation concerning CDD and record keeping, and the prevention and detection of money laundering and terrorist financing (AML/CFT Act, Chapter 3, Section 7, subsection 5, item 2); and
- compliance is monitored by the supervisory authority of the home State of the parent company of the group or consortium (AML/CFT Act, Chapter 3, Section 7, subsection 5, item 3).
- risk management and risk mitigation relating to high-risk states have been appropriately taken into account in the procedures of the group (AML/CFT Act, Chapter 3, Section 7, subsection 5, item 4).

Weighting and Conclusion: There are some deficiencies in the scope of the requirements with regard to the EEA countries.

Recommendation 17 is rated largely compliant.

Recommendation 18 – Internal controls and foreign branches and subsidiaries

In its 3rd MER, Finland was rated partially compliant with these requirements (para. 487-498). The main deficiencies were related to the absence of requirements for money remittance and foreign exchange sectors to develop internal controls or independent audit and have compliance officers; no requirement for non-FIN-FSA-supervised entities to have comprehensive training and employee screening; banks and securities were not required to notify their supervisors when their foreign branches or subsidiaries were prevented by local rules from observing AML/CFT measures. R.18 introduces some new requirements for implementing independent audit functions for internal supervision and AML/CFT programmes for financial groups.

Criterion 18.1 –

(a) Financial institutions are required to have in place policies, procedures and controls that have regard to nature, size and extent of the activities in order to reduce and manage ML/TF risks. The board of directors, active partner or a person holding an equivalent senior management position should approve these policies, procedures and controls, and monitor them. Financial institutions shall designate a person from their management to be responsible for supervising compliance (AML/CFT Act, Chapter 2, Section 3, Chapter 9, Section 1).

(b)-(c) Financial institutions should have procedures in place to ensure that the requirements on staff skills, such as formal qualification and sufficient education and experience, are met at all times. When recruiting new members of staff, financial institutions (with the exception of consumer credit providers, currency exchange providers, and other financial service providers) should pay special attention to their reputation and background (AML/CFT Act, Chapter 9, Section 1; FIN-FSA Regulations and guidelines 8/2014, Section 5.3, para. 18).

(d) Financial institutions should have in place an internal audit, having regard to the size and activities of the entity (AML/CFT Act, Chapter 2, Section 3).

Criterion 18.2 – The provisions of the Section 1, Chapter 9 of the AML/CFT Act are similar to those set out in the elements (a)-(c) of the criterion.

Criterion 18.3 – Branches and majority-owned subsidiaries of the financial groups are required to comply with the home country CDD obligations. When the legislation of the relevant State does not permit compliance with the home country CDD procedures, the financial institution should notify the supervisory authority of this (AML/CFT Act, Chapter 9, Section 2). There is no requirement to apply appropriate additional measures to manage ML/TF risks.

Weighting and Conclusion: There is no requirement to apply appropriate additional measures to manage ML/TF risks when the legislation of a host country does not permit compliance with the home country CDD procedures.

Recommendation 18 is rated largely compliant.

Recommendation 19 - Higher Risk Countries

In its 3rd MER, Finland was rated partially compliant with these requirements (para. 453-456). The deficiencies were related to the absence of formal requirements, and limited possibility to apply counter-measures. R.19 strengthens the requirements to be met by countries and FIs in respect to higher-risk countries.

Criterion 19.1 – Financial institutions are required to apply enhanced due diligence if a customer or a transaction is linked to a State for which this is called for by the European Commission (AML/CFT Act, Chapter 3, Section 10). This falls short of the standard, since the measures should be based on the call by the FATF and since the EC Regulation on high-risk third countries with strategic deficiencies (2016/1675 updated in December 2017) only applies to non EU/EEA states.

Criterion 19.2 – Finland cannot apply countermeasures when it is called upon by the FATF, or independently. It can only do so upon the decision of the European Commission (AML/CFT Act, Chapter 3, Section 10).

Criterion 19.3 – All supervisory authorities (FIN-FSA, Regional State Administrative Agency) have mechanisms in place to inform the supervised entities of countries which are included in the FATF public statements through on-line newsletters.

Weighting and Conclusion: The EDD measures in respect of high-risk third countries may only be applied to non-EEA states. Financial institutions cannot apply countermeasures when it is called upon by the FATF.

Recommendation 19 is rated partially compliant.

Recommendation 20 – Reporting of Suspicious Transactions

In its 3rd MER, Finland was rated largely compliant with these requirements (para. 459-468). The main deficiency was related to the limited obligation to report TF suspicions. There were also concerns about effectiveness, which is not assessed as part of technical compliance under the 2013 Methodology.

Criterion 20.1 – Financial institutions are required to report “any suspicious transaction or suspected terrorist financing” to the FIU without delay (AML/CFT Act, Chapter 4, Section 1). The concept of “suspicious transaction” is very broad, and includes ML and TF-related transactions. “Suspected terrorist financing” is singled out in this provision in order to underline the fact that terrorist-related funds may come from legal sources.

Criterion 20.2 – There are no limitations/ no specific requirements with respect to whether the transaction has been attempted or actually carried out.

Weighting and Conclusion:

Recommendation 20 is rated compliant.

Recommendation 21 – Tipping-off and confidentiality

In its 3rd MER, Finland was rated compliant with these requirements (para. 469 – 471)

Criterion 21.1 – There are no specific rules on immunity in Finnish law, however, the duty to report suspicious transactions to FIU is a *lex specialis*, which means that when a person acts *bona fide* according to law he cannot be held responsible under other provisions of the legal system. In addition, financial institutions are required to “take steps to protect employees” who submit STRs (AML/CFT Act, Chapter 9, Section 1, subsection 2).

Criterion 21.2 – Financial institutions and their employees are prohibited from disclosing the fact that an STR or related information was filed with the FIU (AML/CFT Act, Chapter 4, Section 4, subsection 1).

Weighting and conclusion:

Recommendation 21 is rated compliant.

Recommendation 22 – Designated Non-Financial Businesses And Professions (DNFBPs): Customer Due Diligence

Finland was rated non-compliant with these requirements in its 3rd MER (para. 608-623). The deficiencies noted for FIs in the legal framework also applied to DNFBPs. Trust and company service providers were not covered by AML/CFT provisions. There was a lack of clarity with respect to the AML/CFT obligations for gaming businesses in the Åland Islands. Furthermore, there was no indication that dealers in precious metals and precious stones were complying with their AML/CFT obligations.

Criterion 22.1 – The AML/CFT Act applies equally to FIs and DNFBPs. Therefore, all deficiencies, identified under R.10 with regard to FIs (see above) remain relevant for DNFBPs.

(a) – There are two gambling operators covered by AML/CFT requirements in Finland:

- Veikkaus Oy which is a limited liability company fully owned by the Finland State and has the exclusive right to run gambling (through a mainland and online casino) (AML/CFT Act, Chapter 1, Section 2, Subsection 1, paragraph 9) and
- Penningautomatföreningen, Åland (Paf) (land-based, online and boat-based casino games) (AML/CFT Act, Chapter 1, Section 2, Subsection 1, paragraph 10).

In gambling activities, CDD requirements apply to the two gambling service providers when customers engage in financial transactions (placing of a bet or receive payment of winnings) of EUR 2000 or more whether in a single payment or in several linked payments (AML/CFT Act, Chapter 3, Section 2, Subsection 2).

In addition to the gambling operators, CDD requirements also apply to “traders and corporations supplying registration and charges for participation in gambling provided by the gambling operators ... when the identification and registration of clients has been outsourced by the gambling operator” (AML/CFT Act, Chapter 1, Section 2, Subsection 2).

(b) – Real estate and housing rental agencies are required to comply with all CDD requirements set out in the AML/CFT Act (AML/CFT Act, Chapter 1, Section 2, Subsection 1, paragraphs 18 and 19).

(c) – Dealers in goods (which includes precious metals and stones, see c. 28.2 though) are required to comply with all CDD requirements set out in the AML/CFT Act when they engage in cash transactions equal or above EUR 10.000 (AML/CFT Act, Chapter 1, Section 2, Subsection 1, paragraph 24).

(d) – Advocates and others “providing legal services by way of business or profession” are required to comply with all CDD requirements when they participate whether by acting on behalf of and for their client in any financial or real estate transaction, or by assisting in the planning or carrying out of transactions for their client concerning (AML/CFT Act, Chapter 1, Section 2, Subsection 1, paragraphs 12 and 13):

- buying or selling real property or business entities;
- managing client money, securities or other assets;
- opening or managing bank, savings or securities accounts;
- organising funds for the creation, operation or management of companies; or
- creating, operating or managing foundations, companies or similar corporations.

AML/CFT Act also applies to those performing external accounting functions by way of business or profession regardless of whether they engage in any of the activities set out above.

(e) – Trust and company service providers are required to comply with all CDD requirements set out in the AML/CFT Act when by way of business they provide any of the following services to third parties (AML/CFT Act, Chapter 1, Section 2, Subsection 1, paragraph 21, and Section 4, Subsection 1, paragraph 10):

- the formation of companies;
- acting as a secretary to a company, a partner in a partnership, or a similar position in relation to other legal persons;
- providing a registered office, business or postal address, or other related services;
- acting as a trustee of a foreign express trust referred to in Article 3(7)(d) of the Anti-Money Laundering Directive or similar legal arrangement in Finland;
- acting as a nominee shareholder when the nominee shareholder is entered in the shareholder register of a company other than a public limited liability company.

Criterion 22.2 – All DNFBPs are subject to the same requirements concerning record keeping as FIs as set out in the Accounting Act and AML/CFT Act. Therefore, the same analysis under R.11 (see above) applies.

Criterion 22.3 – All DNFBPs are required to apply the full set of measures concerning PEPs (AML/CFT Act, Chapter 3, Section 13). The legal provisions concerning PEPs apply equally to domestic and foreign PEPs.

Criterion 22.4 – All DNFBPs are subject to a general requirement to carry out an ML/TF risk assessment (AML/CFT Act, Chapter 2, section 3), and in assessing a

customer relationship are obliged to take into account the ML/TF risks relating to new and pre-existing customers, countries or geographic area, products, services, transactions, delivery channels and technologies (AML/CFT Act, Chapter 3, section 1, subsection 2). However, this does not seem to extend to situations when a DNFBP is considering the development of the new product or service *before* the offering to customers. Finland has identified several ML/TF risks related to new products, business practices and technologies, including online gambling (2015 NRA, see c. 1. 1 and 3), but has not assessed those risks. This falls short of the meeting all the requirements of Recommendation 15.

Criterion 22.5 – All DNFBPs are subject to the same requirements concerning reliance on third parties as FIs (AML/CFT Act, Chapter 3, Section 7). Therefore the same deficiencies as identified under R.17 (see above) remain relevant.

Weighting and Conclusion: There are some deficiencies with regard to the scope of the CDD obligations, measures to prevent the misuse of new products, business practices or technologies, and reliance on third parties.

Recommendation 22 is rated largely compliant.

Recommendation 23 - Designated Non-Financial Businesses And Professions (DNFBPs): Other measures

Finland was rated partially compliant with these requirements in the 3rd MER (para. 627-638). The deficiencies noted for FIs in the legal framework also applied to DNFBPs. Trust and company service providers were not covered by AML/CFT provisions. There was a lack of clarity with respect to the AML/CFT obligations for gaming businesses in the Åland Islands. There were also effectiveness issues linked to low number of STRs filed, but this is not assessed as part of technical compliance under the 2013 Methodology.

Criterion 23.1 – All DNFBPs are required to report “any suspicious transaction or suspected terrorist financing” to the FIU without delay (AML/CFT Act, Chapter 4, Section 1), subject to qualifications as set out in c.22.1 (see above).

Traders and corporations supplying registration and charges for participation in gambling provided by the gambling operators may submit STRs through the gambling operator (AML/CFT Act, Chapter 4, Section 1, paragraph 3).

Criterion 23.2 – All DNFBPs are required to implement a risk assessment programme against ML/TF having regard to the ML/TF risks and taking account of the nature, size and extent of the business and its activities which includes

- the development of internal policies, procedures and controls (AML/CFT Act, Chapter 2, Section 3, paragraph 2); and
- “an internal audit when justified with regard to the nature and size of the activities of the obliged entity” (AML/CFT Act, Chapter 2, Section 3, paragraph 2).

In addition to the above risk assessment programme, DNFBPs are required to have in place an ongoing training programme (AML/CFT Act, Chapter 9, Section 1). There are no requirements with regard to screening procedures to ensure high standards when hiring employees. Where the DNFBP is “a part of a group or other conglomerate, it shall comply with the internal policies and guidelines of the group

or other conglomerate issued to ensure compliance with this Act and the provisions issued under it” as well as implement group-wide programmes (AML/CFT Act, Chapter 9, Section 1).

Branches and majority-owned subsidiaries of DNFBPs are required to comply with the home country CDD obligations. When the legislation of the relevant State does not permit compliance with the home country CDD procedures, the DNFBP should notify the supervisory authority of this (AML/CFT Act, Chapter 9, Section 2). This does not include the requirement to apply appropriate additional measures to manage ML/TF risks.

Criterion 23.3 – All DNFBPs are subject to the same requirements concerning high-risk countries as FIs (AML/CFT Act, Chapter 3, Section 10). Therefore the same deficiencies as identified under R.19 (see above) remain relevant. There are no specific mechanisms in place to inform the supervised entities of countries included in the FATF public statements in Åland.

Criterion 23.4 – All DNFBPs are subject to the same requirements concerning tipping-off and confidentiality as FIs (see R.21 above).

Weighting and conclusion: There are deficiencies with regard to screening procedures to ensure high standards when hiring employees. The EDD measures in respect of high-risk third countries may only be applied to non-EEA states. DNFBPs cannot apply countermeasures when it is called upon by the FATF. There are no specific mechanisms in place to inform the supervised entities of countries included in the FATF public statements in Åland.

Recommendation 23 is rated largely compliant.

Recommendation 24 – Transparency and beneficial ownership of legal persons

Finland was rated partially compliant with these requirements in its 3rd MER (para. 663-679). The main deficiencies were the absence of requirements for legal persons to keep or make available information on beneficial ownership or control, limited requirements for legal persons to submit updated information on ownership and control to the trade register, as well as issues of supervision of the existing obligations. New FATF R.24 and its Interpretive Note contain more detailed requirements, particularly concerning the information to be collected on beneficial owners (BO).

Criterion 24.1 –

(a) Different types of legal persons under private law are identified and described in the relevant legal acts:

- limited liability companies (Limited Liability Companies Act);
- partnerships (Partnerships Act);
- co-operatives (Co-operatives Act);
- foundations (Foundations Act);
- associations (Associations Act); and
- religious communities (Freedom of Religion Act);
- mutual insurance company (Insurance Companies Act);
- a savings bank (Savings Banks Act);

- a mortgage society (Mortgage Societies Act);
- an insurance association (Insurance Associations Act);
- a State Enterprise (Act on Unincorporated State Enterprises)⁹⁷;
- a right-of-occupancy association (Act on Right-of-Occupancy Associations);
- branches of foreign legal entities or foundations (Act on the Right to Carry on a Trade; Trade Register Act);
- European Economic Interest Groupings (Act on European Economic Interest Groupings);
- Societas Europaea (Act on Societas Europaea).

(b) The processes for the creation of those legal persons, as well as for obtaining and recording basic and beneficial ownership information are described in the above-mentioned legal acts, Chapter 6 of the AML/CFT Act, as well as on the public websites of the Business Information System (BIS)⁹⁸ and Finnish Patent and Registration Office (PRH)⁹⁹.

Criterion 24.2 – Finland identified ML/TF risks of the misuse of “front companies” in its 2015 NRA (see c. 1.1 and 1.3), however it has not assessed ML/TF risks with regard to legal persons.

Basic information

Criterion 24.3 – All types of legal persons mentioned in c.24.1 have to be registered in the BIS which is administered by the PRH and the Tax Administration (Business Information Act, Section 3). BIS consists of the Trade Register, the Register of Associations, the Register of Foundations and the Register of Religious Communities.

Trade Register contains information about all types of companies (limited liability companies, partnerships, co-operatives, mutual insurance companies, savings banks, mortgage societies, insurance association, branches of foreign legal entities, European Economic Interest Groupings, Societas Europaea), as well as foundations and associations in case they carry out business activities in Finland (Trade Register Act, Sections 1 and 3).

The Trade Register records the company/business name, proof of incorporation, legal form and status, the address of the registered office, and a list of directors (Trade Register Act, Sections 5-13d). Other registers (for foundations, associations and religious communities) record similar information (Foundations Act, Chapter 13, Sections 4 and 5; Associations Act, Section 48; Freedom of Religion Act, Sections 16 and 18). These registers contain information about basic regulating powers (Associations Act, section 48, subsection 2; Freedom of Religion Act, section 18, subsection 2; Foundations Act, Chapter 13, section 2 subsection 1, and section 4). The Articles of Association/rules/statutes pertaining to all types of companies, foundations and associations are registered, as are the natural persons who are authorised to sign on behalf of the applicable legal person (Decree on Trade Register, sections 8, 9, 12, 13).

⁹⁷ As its beneficial owner is in practice the Finnish state, this type of legal person will not be considered for the purposes of R.24.

⁹⁸ www.ytj.fi

⁹⁹ www.prh.fi

Information in the Trade Register, the Register of Foundations, the Register of Associations and the Register of Religious Communities set out above is public (Trade Register Act, Section 1a; Foundations Act, Chapter 13, Section 1; Associations Act, Section 47). There is no specific provision stipulating public access to the information held in the Register of Religious Communities. However, under the Finnish publicity legislation, any information which is not specifically indicated as “not public” is considered public.

Criterion 24.4 – All legal persons are required to submit basic information set out in c.24.3 to one of the public registers (see above). They are also required to keep that information together with accounting records (Accounting Act, Section 1).

Limited liability companies, mutual insurance companies and Societas Europaea have to maintain the register of shareholders containing the number of shares and categories of shares, which has to be kept at the head office (Limited Liability Companies Act, Chapter 3, Sections 15 and 17, Insurance Companies Act, Chapter 4, section 1, Act on Societas Europaea, Section 1, Subsection 2 and Council Regulation (EC) No 2157/2001, Article 9). Cooperatives are required to maintain a list of their members at the head office of the cooperative (Cooperatives Act, Chapter 4, Sections 14 and 16). Savings banks are required to maintain a list of shares and keep it in the main office (Act on Savings Banks, Chapter 2, section 20, subsections 1 and 2). Insurance associations are required to keep a list of holders of the guarantee shares at the main office (Act on Insurance Associations, Chapter 3, section 10, subsections 1 and 2, and section 12). Right of occupancy associations, associations and religious communities have to maintain the list of their members (Act on Right of Occupancy Associations, section 10; Associations Act, Section 11; Freedom of Religion Act, Section 11), but there are no specific requirements with regard to the location where this information should be maintained. Partnerships and foundations are required to submit a partnership agreement/foundation charter which contains a list of partners/founders (Partnerships Act, Chapter 1, Section 4; Act on Foundations, Chapter 2, Section 1) to the Trade Register and Register of Foundations, accordingly.

Mortgage societies and European Economic Interest Groupings are not required to maintain the list of the members respectively.

Criterion 24.5 – All legal persons are required to notify any changes with regard to the information submitted to the BIS without delay (Business Information Act, Section 11 and Trade Register Act, Section 14).

The PRH is empowered, but not required, to update its records and check the personal information contained in the submissions against information of the Population Register Centre in order to verify their accuracy (Trade Register Act, Section 21a).

All share acquisitions have to be entered in the share register without delay (Limited Liability Companies Act, Chapter 3, Section 16). Cooperatives are required to maintain the list of their members up-to-date (Cooperatives Act, Chapter 4, Section 14).

Since partnerships are required to submit a partnership agreement which contains a list of partners (Partnerships Act, Chapter 1, Section 4) to the Trade Register, they are consequently required to notify any changes to it without delay (Trade Register Act, Section 14).

According to the Foundations Act, the by-laws of a foundation (Foundations Act, Chapter 6, section 1) and the purpose of the foundation (Foundations Act, Chapter 6, section 2) may be amended. This has to be notified to the Register without delay (Foundations Act, Chapter 13, section 6). However, the founding deed of a foundation (concerning e.g. the founders of the foundation) cannot be changed after the registration of a foundation. Thus, the requirement to update this information does not apply.

There are no requirements to update any changes to or keep the list of shareholders/partners/members or authorised signatories for savings banks, mortgage societies, insurance associations, right-of-occupancy associations, European Economic Interest Groupings, associations and religious communities up-to-date.

Beneficial Ownership Information

Criterion 24.6 – 24.7 There are no requirements concerning availability of beneficial ownership of companies.¹⁰⁰ However, competent authorities may rely on the existing information held by financial institutions and DNFBPs (see R.10 and 22).

In case of associations, limited liability housing and property companies, the members of board of directors are deemed by law to be the beneficial owners (AML/CFT Act, Chapter 1, Section 7). Similarly, for foundations, the members of the board of trustees and the supervisory board are deemed by law to be the beneficial owners. Given the particularity of these types of legal persons (no ownership, or very dispersed ownership and control structures) this approach is in line with the FATF definition. As mentioned above, members of the board and the supervisory board are recorded in the relevant registries; hence the information on the beneficial owners for these types of legal persons is available.

Criterion 24.8 – There is a requirement that at least one of the members of the board of directors/partners shall be resident within the European Economic Area, unless the registration authority grants an exemption to the company (Limited Liability Companies Act, Chapter 6, Section 10; Freedom of Enterprise Act, Section 1, Paragraph 2; Co-operatives Act, Chapter 6, Section 10, Foundations Act, Chapter 3, Sections 10, 17 and 22, Associations Act, Section 35). Should an exemption be granted, the company shall have a separate representative resident in Finland (Act on the right to carry on a trade, Section 6, subsection 3). This falls short of the requirement for the person to be resident in the country, moreover there is a possibility of an exemption.

There is no general requirement to cooperate with the competent authorities. The FIU has the right to obtain from companies any information necessary to exercise its duties (FIU Act, Section 4), and police have wide powers to obtain any information needed for investigation (Police Act, Chapter 4, section 3; Coercive Act, Chapter 7, section 1). Those legal persons that are obliged entities under the AML/CFT Act have an obligation to cooperate with the supervisors

¹⁰⁰ The relevant provisions of the AML/CFT Act (Chapter 6, Section 2 and 3) which introduce a register of beneficial owners will enter into force on 1 January 2019 and therefore are not taken into account for the purposes of TC analysis.

Criterion 24.9 – When operations of a legal person are terminated, the legal person or the beneficiary must arrange retention of the accounting material (financial statements, management report, ledgers, chart of accounts and the list of ledgers and materials) for at least 10 years (Accounting Act, Chapter 2, section 10). That does not seem to include basic and beneficial ownership information.

However, any data registered in the Trade register (and other registers as mentioned in 24.3) is maintained permanently in electronic form, as decided by the Archive Institute on 27 October 2015 in accordance with the authority given to it by the Section 8 of the Archive Act.

For the record-keeping obligations of the FIs and DNFBPs, please refer to R.11 and R.22.

Criterion 24.10 – Access to the basic information submitted to the BIS is public and on-line (see above). Police and FIU have the right to request and obtain any basic information from companies, as well as beneficial ownership information from FIs (Police Act, Chapter 4, section 3; FIU Act, section 4). However there are no requirements with regard to the timeframe within which this information should be provided. FIN-FSA and RSAA have the right to obtain, for carrying out a specific supervisory measure, any information that is necessary for the exercise of supervision from an auditor and any other person in relation to an entity or participant subject to its supervision (FIN-FSA Act, Chapter 3, Section 19, AML/CFT Act Chapter 7, Section 2). The Tax Administration has the power to obtain information on companies for the purposes of taxation, under the Act on Taxation Procedure (Act on Taxation Procedure, Sections 11, 14, 19, and 21). This includes basic information with regard to company shareholders, and “deemed” beneficial owners being persons registered as members of the board of directors of the legal person, but only to the extent the legal person is holding it. It is not expressly provided for that the Tax Administration may call for beneficial ownership information of any legal person.

Criterion 24.11 - Bearer shares are not allowed by the virtue of the provisions of the Chapter 3, section 10, subsection 1 of the Limited Liability Companies Act, according to which “a share certificate shall be issued only to a specified person”. This provision has been in force since 1 January 1980. Finland acknowledges that a marginal number of companies that were established and incorporated before that time according to the 1895 Limited Liability Companies Act may still have bearer shares in circulation. There are no legislative or administrative measures in place to convert bearer shares to nominal or ordinary shares.

Criterion 24.12 There is no direct prohibition on nominee directors. Nor are there obligations to disclose the identity of, or license the nominator, record the nominee status and make such disclosure in the company registry and/or relevant registry, maintain such information, or make it available to competent authorities upon request. However, in accordance with the general principles of the Limited Liability Companies Act, the Board membership (including the duties and responsibilities relating to it) is personal and cannot be transferred upon another person (nor may the General Meeting authorise a member of the Board of Directors to transfer the duty to another person).

There is no explicit prohibition on nominee shareholders. Nor are there obligations to disclose the identity of or license the nominator, record the nominee status and make such disclosure in the company registry and/or relevant registry, maintain such information, or make it available to competent authorities upon request. Nominees are allowed in the cases of custodial account of the Book-Entry System. In that case, the nominee has an obligation to notify the FIN-FSA of the name of the beneficial owner of the book entries, where this is known, and the number of the book entries held by the owner (Act on the Book-Entry System and Settlement Activities, Chapter 4 section 4).

Criterion 24.13 – Anyone who intentionally or through negligence fails to submit the necessary information to the BIS is liable to a penal fine (Business Information Act, Section 19). The amount of the fine is not expressly defined, but it is based on the disposable income of the offender. The minimum amount of the day fine is set at EUR 6 (Decree on the Amount of the Day Fine, Section 5) and the maximum number of day fines that can be imposed is 240. These sanctions cannot be considered as proportionate and dissuasive (especially in cases of the so-called “straw men” who usually do not have any disposable income at all – in this case the maximum amount of fine would be 6x240= EUR 1 440).

Intentional submission of incorrect information to any public register is subject to a fine or to imprisonment for up to three years (Criminal Code, Chapter 16, section 7). This sanction appears to be proportionate and dissuasive.

Failure to keep a shareholder register in case of limited liability companies, mutual insurance companies and Societas Europaea is subject to a fine (Limited Liabilities Companies Act, Chapter 25, Section 2, Insurance Companies Act, Chapter 29, section 5). The amount of the fine is not specified. Similar sanctions apply to co-operatives (Co-operatives Act, Chapter 27, Section 2).

Insurance associations are subject to a fine for a failure to maintain the list of holders of the guarantee shares (Act on Insurance Associations. Chapter 16, section 9). The amount of the fine is not specified.

Right of Occupancy Associations are subject to a fine for a failure to maintain a list of members (Act on the Right of Occupancy Associations, section 83). The amount of the fine is not specified.

There are no sanctions available for breaching the obligation to maintain and keep updated lists of shareholders/members/partners of associations and religious communities, savings banks, and mortgage societies.

FIN-FSA has the right to impose conditional fines in for breaching the obligation to provide information under AML/CFT Act (AML/CFT Act, Chapter 7, Section 7). There are no sanctions available for breaching the obligations to provide information to other competent authorities.

Criterion 24.14 –

(a) Insofar as basic information is available in the public commercial register (see c. 24.3), it can also be accessed by foreign competent authorities (by virtue of its public nature).

(b) Information on shareholders may be exchanged by the FIUs and law enforcement authorities through their channels of cooperation (see R. 40).

(c) The FIU and law enforcement authorities have investigative powers to obtain beneficial ownership information (to the extent that it is available in Finland) on behalf of their foreign counterparts (see R.37 and 40).

Criterion 24.15 – There is no legal requirement to monitor the quality of assistance received from other countries in response to requests for basic and beneficial ownership information or requests for assistance in locating beneficial owners residing abroad. This is done within the framework of regular case management by the FIU and the NBI.

Weighting and Conclusion: The main deficiency is the absence of a general requirement to keep accurate and up-to-date information on the beneficial owners of the legal persons in Finland. There are also some deficiencies with regard to scope of requirements to maintain basic information for certain types of legal persons. There is no requirement to disclose nominee shareholders and directors and record their status in registries. Timely access to ownership information by competent authorities is not formally stipulated. There are some gaps in the obligations placed on officers of the legal entities to cooperate with authorities in all circumstances. There are gaps in sanctions available for the breaches of information keeping requirements.

Recommendation 24 is rated partially compliant.

Recommendation 25 - Transparency and beneficial ownership of legal arrangements

In the 3rd MER, these requirements were not considered to be applicable to Finland (para. 682-683). The revised Recommendation (R. 25) is applicable to all countries, including those that do not recognise trusts.

Criterion 25.1 –

(a)-(b) Express trusts or other comparable legal arrangements cannot be established under the Finnish law.

(c) Finnish professional trustees for trusts or other comparable legal arrangements governed under foreign law are subject to AML/CFT Act, and as such are required to undertake CDD measures and retain CDD data for at least 5 years (AML/CFT Act, Chapter 1, Sections 2 and 6, Chapter 3, Section 3 and 6).

Criterion 25.2 – All obliged entities (which include FIs, professional trustees and other DNFBPs) have to maintain accurate and up-to-date information about settlor or protector, trustee, or beneficiaries of a trust (AML/CFT Act, Chapter 3, Section 6).

Criterion 25.3 – Although subject to the AML/CFT Act, there are no specific provisions requiring trustees to disclose their status as trustees of a foreign express trust or any trust to FIs and DNFBPs. However, the status would be checked as part of the CDD obligations by the obliged entity which is entering into a business relationship with the trustee (see R.10 and R.22 above).

Criterion 25.4 – There are no legal provisions in the Finnish law or other enforceable means that would prevent the trustees from disclosing any information relating to the trust.

Criterion 25.5 – Law enforcement authorities have all necessary powers to obtain timely access to information held by trustees, other DNFBPs and FIs (see c.31.1).

This includes all information that FIs, trustees and other DNFBs collect as part of the CDD process (see R.10 and R.22), including beneficial ownership, residence of the trustee and assets managed by them. FIN-FSA and RSAA have similar powers (FIN-FSA Act, Chapter 3, sections 18 and 19; AML/CFT Act, Chapter 7, section 2).

Criterion 25.6 –

(a) Express trusts or other comparable legal arrangements cannot be established under the Finnish law, therefore this requirement is not applicable.

(b) Domestically available information on the trusts or other legal arrangement held by Finnish trustees may be exchanged by the FIUs and law enforcement authorities through their channels of cooperation (see R. 40).

(c) The FIU and law enforcement authorities can use investigative powers to obtain beneficial ownership information (to the extent that it is available in Finland) on behalf of their foreign counterparts (see R. 37 and R.40).

Criterion 25.7 – Trustees are legally liable for any failure to perform the duties relevant to meeting their obligations and they are subject to sanctions such as administrative fines (up to EUR 100 000 for legal persons, up to EUR 10 000 for natural persons), penalty payments (up to two times the gain resulting from the act or omission, or EUR 1 million, whichever is higher), public warnings (AML/CFT Act, Chapter 8, Sections 1-3, and 5). These sanctions appear to be proportionate and dissuasive.

Criterion 25.8 – The information about trusts referred to in c. 25.1 may only be held by the obliged entities which are subject to AML/CFT Act. The supervisory authorities (FIN-FSA and RSAA) may impose a conditional fine for the breach of the obligation to grant timely access to that information (AML/CFT Act, Chapter 7, section 7). The amounts of such fines are not defined, but they are based on the disposable income of the offender. When considering the amount of conditional fine, the nature and extent of primary obligation, financial standing and other facts that have relevance should be taken into consideration (Act on Conditional Fines, Section 8). The minimum amount of the day fine is set at EUR 6, but can go up to EUR 40 million in practise. This appears are proportionate or dissuasive.

Weighting and Conclusion: There are no specific provisions requiring trustees to disclose their status as trustees of a foreign express trust or any trust to FIs and DNFBPs.

Recommendation 25 is rated largely compliant.

Recommendation 26 – Regulation and supervision of financial institutions

Finland was rated partially compliant with these requirements in its 3rd MER (para. 505-590). The main deficiencies were related to the absence of supervisor for the money exchange and remittance sectors, and absence of provisions to prevent criminals from holding a controlling interest in institutions operating in the money exchange or remittance sectors. There were also effectiveness concerns, which are not assessed as part of technical compliance under the 2013 Methodology. The new R. 26 strengthens the principle of supervision and controls, in accordance with a risk-based approach.

Criterion 26.1 – There are two supervisors responsible for regulating and supervising financial institutions' compliance with the AML/CFT requirements, the Financial Supervisory Authority (FIN-FSA) and the Regional State Administrative Agency (RSAA).¹⁰¹ RSAA supervises only (i) consumer credit providers, (ii) currency exchange providers, and (iii) other financial service providers (which includes granting of credits and financing activity as well as other arrangement of financing; financial leasing; and guarantee operations), while FIN-FSA is responsible for the rest of the financial institutions (AML/CFT Act, Chapter 7, section 1; FIN-FSA Act, Chapter 1, section 3; Government Decree on Regional State Administrative Agencies (906/2009), Section 9).

Criterion 26.2 – All Core Principles financial institutions are required to be licensed by:

- the ECB (Act on Credit Institutions, Chapter 2, Section 1, Chapter 4, Sections 1-2; Council Regulation (EU) No 1024/2013, Articles 4 and 14; Regulation (EU) No 468/2014, Articles 73-78) and
- the FIN-FSA (Act on Credit Institutions, Chapter 17, Section 2; Insurance Companies Act, Chapter 1, section 13 and Chapter 2, Section 18b; Act on Foreign Insurance Companies, Chapter 4, Section 18; Act on Common Funds, Chapter 2, Section 5 a, subsection 1 and Section 9; Act on Investment Services, Chapter 2, Section 1, Chapter 3, Section 1 and Chapter 5, Section 1).

Other financial institutions are required to be either licensed or registered by:

- the FIN-FSA (Act on Payment Institutions, Chapter 2, Section 6, Subsection 1, Sections 7, 7a and 8; Act on Alternative Investment Fund Managers, Chapter 1, Sections 2-3, Chapter 3, Section 1 and Chapter 5, Section 1; Act on Insurance Mediation, Chapter 2, Section 5; Act on Intermediaries of Consumer Credit Relating to Residential Property, Section 3; Crowdfunding Act, Section 3; Local Mutual Insurance Associations Act, Chapter 1, Section 1 and Chapter 2, Sections 4 and 10);
- the Ministry of Finance (Act on the Book Entry System and Settlement Activities Chapter 2, Section 1 and Section 23; Act on Trading in Financial Instruments, Chapter 2, Section 1);
- the RSAA (Act on the Registration of Certain Credit Providers and Credit Intermediaries, Section 3; AML/CFT Act, Chapter 9, Section 8 by virtue of applying Section 27 of the repealed AML/CFT Act of 2008.)¹⁰²

Companies providing other financial services (e.g. non-consumer loans, financial leasing) were not subject to registration or licencing as of the end of the on-site visit.

¹⁰¹ There are six Regional State Administrative Agencies in Finland which correspond to the administrative divisions of the country. However, the registration and supervision duties based on the AML/CFT Act are designated to the RSAA for Southern Finland in respect of all regions (Government decree on Regional State Administrative Agencies, Section 9, Subsection 1, paragraph 2).

¹⁰² Please note that this requirement had not existed before 05.06.2018 and de-facto was not yet implemented at the time of the on-site visit (June 2018).

There is no formal prohibition on the establishment or continued operation of shell banks. However, it is required in the Act on Credit Institutions, Chapter 5, Section 9 that a credit institution shall have its main office and at least one fixed place of business in Finland. The conditions for licensing, set out in the law, do not make it possible to establish a shell bank in Finland. The Decree of the Ministry of Finance (697/2014) lays down the documents and clarifications to be appended to an application for authorisation including, among other things, the address of an office in Finland for the purpose of its business operations, although there is no requirement to have meaningful mind and management located within Finland. The only requirement is to have at least one of the members of its Board of Directors as well as its Managing Director as a permanent resident in the EEA (Act on Commercial Banks and Other Credit Institutions in the Form of a Limited Company, Chapter 1, Section 2). In case of a branch of a third-country credit institution, the director and other responsible persons shall be resident in Finland (Act on Credit Institutions, Chapter 18, Section 10, subsection 4).

Criterion 26.3 –

For credit institutions, the competent authority to prevent criminals or their associates from owning financial institutions as well as for authorisations is the ECB. An initial application for license or acquisition of qualifying holdings is submitted to FIN-FSA who carries out preliminary assessment of all material submitted. The FIN-FSA prepares a draft proposal which is sent to ECB. The final decision is taken by the ECB (Council Regulation (EU) No 1024/2013, Article 4, 14 and 15).

As of time of the assessment, there were three significant supervised entities: Kuntarahoitus Oyj, Nordea Bank AB (publ), Finnish Branch and OP Osuuskunta. For these entities, the ECB is also the competent authority to decide on the fit and properness of the managers. In its decisions regarding fit and properness of the owners and managers of financial institutions, the ECB is guided by the national legislation (Council Regulation (EU) No 1024/2013, Article 4, para.3). The national framework is explained below.

For financial institutions, the precondition for the granting of an authorisation (a license) is that the major owners (both through direct and indirect holdings) and the management of a FI applying for authorisation are reliable (Act on Credit Institutions, Chapter 4, Sections 1 and 3-4, Chapter 7, Section 4, Chapter 17, Sections 2-3; Act on Common Funds, Chapter 2, Sections 5a, 5b, 5e, 5f, 9a, 9d and 9e; Act on Investment Services, Chapter 3, Sections 3 and 4, Chapter 5, Sections 1-3, Chapter 6b, Section 4; Commission Delegated Regulation (EU) 2017/1943, Article 9; Act on Payment Institutions Chapter 3, Sections 13 and 13 a, Chapter 4, Section 25; Act on Alternative Investment Fund Managers Chapter 4, Sections 3-4, Chapter 6, Section 5, Chapter 14, Sections 6 and 8-9, Insurance Companies Act, Chapter 2, Section 3, Section 6, Chapter 4, Sections 5-6 and Chapter 6, Sections 4-5, and Section 9; Commission Delegated Regulation (2015/35) Article 273, Article 318 and Articles 322-323; FIN-FSA Regulations and Guidelines 6/2015 Commencement of operations and the governance system of a life and non-life insurance company, Chapter 4.5 and Chapter 9; Act on Foreign Insurance Companies Sections 19-20 and Section 24; Act on the Book-Entry System and Settlement Activities Chapter 1, Section 1 and Chapter 2, Sections 1 and 23; CSD Regulation (EU) 909/2014 Article 27; EMIR Regulation (EU) 648/2012, Articles 27 and 30).

Generally the precondition for the registration is that the major owners and the management of a FI applying for registration are reliable (Act on Intermediaries of Consumer Credit Relating to Residential Property, Sections 5-7; Crowdfunding Act, Sections 4 and 6-7; Act on the Registration of Certain Credit Providers and Credit Intermediaries, Sections 4 and 6; AML/CFT Act, Chapter 9, Section 8 by virtue of applying Section 27 of the repealed AML/CFT Act of 2008). For payment service providers without an authorisation (registered entities) and insurance intermediaries the reliability requirements only apply to the management, but not the owners (Act on Payment Institutions, Chapter 2, Sections 7, 7a, 7b, 8 and Chapter 3, Section 13a; Act on Insurance Mediation Chapter 2, sections 6-7 and 11).

Reliability requirements include the absence of an imprisonment sentence in the five years preceding the evaluation or the absence of a fine related to a crime committed in the three years preceding the evaluation (Act on Credit Institutions, Chapter 7, Section 4; Act on Common Funds, Sections 5e, 9d; Act on Investment Services, Chapter 6b, Section 4; Act on Payment Institutions, Section 25; Act on Alternative Investment Fund Managers, Chapter 6, Section 5, Chapter 14, Section 8; Act on Insurance Mediation, Chapter 2, Section 11; Act on Intermediaries of Consumer Credit Relating to Residential Property, Section 7; Crowdfunding Act, Section 7; Act on the Registration of Certain Credit Providers and Credit Intermediaries, Section 5; AML/CFT Act, Chapter 9, Section 8 by virtue of applying Section 27 of the repealed AML/CFT Act of 2008).

There are notification obligations regarding changes in the management and major holdings, which will take place after authorisation or registration (FIN-FSA Act, Section 5, paragraph 10, Act on Credit Institutions, Chapter 3, Section 1, Chapter 4, Section 1 and Chapter 7, Section 4; Act on Common Funds, Chapter 2, Sections 5e, 9d, 10b and 16; Act on Investment Services, Chapter 3, Section 8, Chapter 6a, Section 1 and Chapter 6b, Section 4; Act on Payment Institutions, Chapter 2, Section 8, Chapter 3, Section 11 and Chapter 4, Sections 21a and 21c; Act on Alternative Investment Fund Managers, Chapter 4, Section 5, Chapter 6, Section 5, Chapter 7, Section 9 and Chapter 14, Section 10; Articles 16 (3-4) and 27 (7) of the CSD Regulation (EU) 909/2014); Act on Intermediaries of Consumer Credit Relating to Residential Property, Section 9; Crowdfunding Act, Section 5; Act on Insurance Mediation Chapter 2, Section 9; AML/CFT Act, Chapter 9, Section 8 by virtue of applying Section 29 of the repealed AML/CFT Act of 2008; Insurance Companies Act, Chapter 4, Section 5; Chapter 6, Sections 4-5 and 9; Local Mutual Insurance Associations Act, Chapter 6, Section 3; EMIR Regulation (EU) 648/2012, Article 31).

Supervisory authorities may prohibit a person from acting as a member or deputy member of the board of directors of an obliged entity or as the managing director, deputy to the managing director or other member of senior management in an obliged entity for a period not exceeding five years (AML/CFT Act, Chapter 7, Section 5; FIN-FSA Act, Section 28; AML/CFT Act, Chapter 9, Section 8 by virtue of applying Sections 27 and 30 of the repealed AML/CFT Act of 2008) if:

- the person has demonstrated obvious incompetence or carelessness in the performance of duties and it is apparent that this may seriously jeopardise the achievement of the objectives provided in this Act; or
- the person does not satisfy the professional competence and reliability requirements separately provided by law.

RSAA may prohibit a person in the employ of a party engaging in the provision of consumer credit and the mediation of peer-to-peer lending or another person acting on account of that party (Act on the Registration of Certain Credit Providers and Credit Intermediaries, Section 17). RSAA may also refuse registration if, taking into account the circumstances, it is apparent that the person applying for registration intends to engage in the provision of consumer credit or the mediation of peer-to-peer lending as a go-between for a third party (Act on the Registration of Certain Credit Providers and Credit Intermediaries, Section 4).

FIN-FSA has the right to prohibit acquisition of a holding in a financial institution on the grounds that there is justifiable cause to suspect (FIN-FSA Act, Section 32a) that:

- the reputation of the entity subject to the notification requirement is compromised or its financial position is inadequate;
- the fitness and propriety of the management of the target company or corporation, or other authorisation criteria, would be jeopardised by the acquisition;
- supervision of the target company or corporation and related information sharing between the authorities would be jeopardised by the acquisition; or
- the acquisition is related to money laundering or the financing of terrorism.

FIN-FSA has also the powers to restrict the use of the voting rights related to major owners, which had acquired the shares earlier and then assessed to be fit & proper, but later turned out to be unfit or improper (FIN-FSA Act, Section 32c).

For certain types of financial institutions there are restrictions on persons who own 10 or more percent of shares which involve absence of imprisonment sentence in the five years prior to the acquisition, or a fine to a crime in the three years preceding the acquisition (Act on Credit Institutions, Chapter 3, Section 2; Act on Common Funds, Section 5f, 9e; Act on Investment Services, Chapter 3, Section 4; Act on Payment Institutions, Section 13a; Act on Alternative Investment Fund Managers, Chapter 4, Section 4, Chapter 14, Section 9; Act on Intermediaries of Consumer Credit Relating to Residential Property, Section 7; Crowdfunding Act, Section 7).

In assessing the reliability of managers and owners of the financial institutions FIN-FSA shall also take into account their close links with other natural and legal persons in order to prevent associates of criminals from holding managerial positions and becoming owners of financial institutions (Act on Credit Institutions, Chapter 5, Section 12; Insurance Companies Act, Chapter 1, Section 10, Chapter 2, Section 8; Act on Common Funds, Chapter 2, Sections 5b and 10b; Act on Alternative Investment Fund Managers, Chapter 4, Section 3; Act on Investment Services, Chapter 1, Section 26, paragraph 15, and Chapter 7, Section 4; Act on Payment Institutions Chapter 4, Section 21; and the Act on the Book-Entry System and Settlement Activities, Chapter 2, Section 11; Act on Intermediaries of Consumer Credit Relating to Residential Property, Section 6; Local Mutual Insurance Associations Act, Chapter 2, Section 5b; Crowdfunding Act, Section 6; AML/CFT Act, Chapter 9, Section 8 by virtue of applying Section 27 of the repealed AML/CFT Act of 2008).

There are no precise reliability requirements for the managers and owners of insurance companies, local mutual insurance associations, a central securities depository and a central counterparty, as well as companies providing other financial services (e.g. non-consumer loans, financial leasing), although there are general principles referring to a good repute for most of sectors. They are not specific enough to satisfy fit-and-proper requirements of criterion 26.3.

Criterion 26.4 – (Met)

(a) Banking, securities, and insurance institutions are regulated and supervised in line with Core Principles, where relevant for AML/CFT, including the application of consolidated group supervision for AML/CFT purposes.¹⁰³

(b) Other financial institutions are regulated and supervised for compliance by FIN-FSA and RSAA having regard to ML/TF risks (AML/CFT Act, Chapter 2, section 2). MVTS providers are also regulated and supervised for compliance (see R.14).

Criterion 26.5 – When determining the scope and frequency of supervision, the supervisors should have regard to (i) ML/TF risks concerning the supervised sector, supervised entities and their customers, products and services; (ii) the ML/TF risk assessments prepared by them (which in turn should be based on national and European-wide assessments); and (iii) exemptions applicable to the activities of supervised entities (AML/CFT Act, Chapter 2, section 2).

Criterion 26.6 – The supervisors are required to update their risk assessments (which include entity-specific assessments) on a regular basis and in case of material events or changes in the activities of the supervised entities (AML/CFT Act, Chapter 2, section 2).

Weighting and Conclusion: The provisions of Recommendation 26 are met for most types of financial institutions. The exceptions are companies providing other financial services (e.g. non-consumer loans, financial leasing) who are not subject to registration or licencing. Furthermore, there are no specific fit-and-proper requirements for the managers and owners of insurance companies, local mutual insurance associations, a central securities depository and a central counterparty, as well as companies providing other financial services.

Recommendation 26 is rated largely compliant.

Recommendation 27 – Powers of supervisors

Finland was rated partially compliant with these requirements in its 3rd MER (para. 528-559), mainly for effectiveness reasons. Effectiveness is not assessed as part of technical compliance under the 2013 Methodology. The new R. 27 extends the range of disciplinary and financial sanctions powers which the supervisors should have, including the power to withdraw the licenses of FIs.

Criterion 27.1 – FIN-FSA and RSAA have the authority to supervise and ensure compliance by financial institutions with AML/CFT requirements (AML/CFT Act, Chapter 7, section 1). However, they do not have statutory powers to carry out the

¹⁰³ See November 2016 IMF FSAP report (www.imf.org/~media/Files/Publications/CR/2017/cr1703.ashx)

supervision of the implementation of the targeted financial sanctions obligations (see R. 6).

Criterion 27.2 – The supervisors have the right to conduct inspections of financial institutions. This includes the right to obtain access to the documents and other records and information systems to the extent necessary to perform supervisory duties (AML/CFT Act, Chapter 7, section 3; FIN-FSA Act, Chapter 3, section 24). In the case financial institutions use residential premises for the conduct of business activities, the powers of the supervisors to conduct inspections is limited to those instances only when there is justified cause to suspect that the obliged entity has, wilfully or negligently, seriously, repeatedly or systematically neglected or violated AML/CFT Act. Given that there are no restrictions for using residential premises for business purposes, this precondition makes it impossible to conduct routine on-site inspections.

Criterion 27.3 – Financial institutions are obliged without undue delay and free of charge to supply the supervisors with all information and reports requested by them (AML/CFT Act, Chapter 7, section 2). Also, FIN-FSA has the right to obtain information from auditors, and “*persons ... who, with justifiable cause, may be presumed to have information necessary for carrying out such supervisory measures*”, from the register of fines and the criminal record, from criminal investigation and prosecuting authorities, and other Finnish undertakings as belonging to the same conglomerate as a supervised entity (FIN-FSA Act, Chapter 3, section 18, 19, 20, 23).

Criterion 27.4 – For breach of AML/CFT Act, the supervisors are authorised to impose sanctions, such as administrative fines (up to EUR 100.000), penalty payments (up to 10% of the groups turnover or EUR 5 million, whichever is higher) which may also be applied to a member of the management, public warnings (AML/CFT Act, Chapter 8, sections 1-4), as well as temporary restrictions of activities of financial institutions’ management (AML/CFT Act, Chapter 7, section 5; FIN-FSA Act, Chapter 3, section 28).

In case of material breach of the provisions governing financial markets or the provisions or regulations issued thereunder by the authorities (which includes AML/CFT), FIN-FSA has the right to withdraw license or, if it was granted by the ECB or another competent authority, propose withdrawal of license to such other authority (FIN-FSA Act, Chapter 3, section 26), and restrict activity of financial institutions (FIN-FSA Act, Chapter 3, section 27). The RSAA has powers to cancel registration of consumer credit providers and peer-to-peer lending intermediaries (Act on the Registration of Certain Credit Providers and Credit Intermediaries, section 18). Ministry of Finance has the powers to revoke the authorisations for CSD and CCPs as well as stock exchange (Regulation (EU) No 909/2014, Article 20; Regulation (EU) No 648/2012, Article 20, Act on Trading in Financial Instruments, Chapter 2, Section 14) by virtue of being the competent authority referred in the relevant EU Regulations.

Since supervisors do not have statutory powers to carry out the supervision of the implementation of the targeted financial sanctions obligations (see c. 27.1) there is no sanction applicable in practice.

Weighting and Conclusion: The supervisors do not have statutory powers to carry out the supervision of the implementation of the targeted financial sanctions obligations. The powers of the supervisors to conduct inspections are limited when

financial institutions use residential premises for the conduct of business activities. There are no sanctions applicable for violation of targeted financial sanctions obligations.

Recommendation 27 is rated partially compliant.

Recommendation 28 – Regulation and supervision of DNFBPs

Finland was rated non-compliant with these requirements in its 3rd MER (para. 640-653). The new FATF requirements strengthen the risk-based approach to regulation and supervision of DNFBPs.

Criterion 28.1 – The casino situated on the mainland in Finland and online casinos offering their services to mainland Finland residents fall in the scope of the Lotteries Act. The gambling facility (Paf Casino) situated on the Åland Islands, casino games aboard ships registered on Åland as well as online casinos offering services to the residents of Åland are authorised in terms of the Åland Regional Lotteries Act.

(a) Mainland casinos (brick-and-mortar and online) are required to be authorised by law (Lotteries Act, Chapter 2, Section 6), which is equivalent to the requirement of licensing. Veikkaus Oy has the exclusive right to operate casinos in mainland Finland (Lotteries Act, Chapter 3, Section 11).

Gambling operators in Åland are required to be licensed, and they have to be established as public law association by means of a regional decree (Åland Regional Lotteries Act, Section 3; Regional Decree on Ålands Penningautomatförening and its activities).

(b) Veikkaus Oy (mainland casinos) is a limited liability company fully owned by the State (Lotteries Act, Chapter 3, Section 12). There are general provisions concerning limited liability companies which prohibit persons who are bankrupt or have been found guilty of criminal conduct in the course of the company's business activities from serving as board members (Limited Liability Companies Act, Chapter 6, section 10, Act on Business Prohibitions), but these provisions fall short of the requirement to *prevent* criminals and *their associates* from serving as board members. There are no specific provisions applicable to the people in charge of the operational management of the casino.

Paf is an association, the activities of which are governed by regional decrees. The Government of Åland is responsible for appointing board members of the association and may release individual members from their duties (Regional decree amending the decree on Penningautomatförening Åland and its activities, Section 7). There are no requirements to prevent criminal or their associates from being the board members. There are no provisions applicable to the people in charge of the operational management of the gambling operators.

(c) Mainland casinos and gambling operators in Åland are subject to nominal AML/CFT supervision by the National Police Board (AML/CFT Act, Chapter 7, Section 1, subsection 1, item 2). The NPB was a nominal designated AML/CFT supervisor of Åland gambling operator Paf for one month (June 1st 2018 - June 30th

2018). It has not exercised in practise any supervisory powers over Paf under the AML/CFT Act.¹⁰⁴

Criterion 28.2 – Regional State Administrative Agency (RSAA) is responsible for monitoring and ensuring compliance of real estate agents in mainland Finland, dealers in goods paid in cash above EUR 10,000 which includes precious metals and stones, legal professionals other than advocates, trust and company service providers, as well as external accountants (AML/CFT Act, Chapter 7, Section 1, subsection 1, item 4). All dealers in precious metals and stones are included in the concept of “dealers in goods” and thus are subject to the AML/CFT Act.

Finnish Bar Association is responsible for monitoring and ensuring compliance of advocates (AML/CFT Act, Chapter 7, Section 1, subsection 2).

The Åland Government supervises compliance of real estate agents with the provisions of the Regional Decree on real estate agents 1996:48 (Section 17), which mainly govern the access to the profession and business operations. The Åland Government’s supervision powers do not include AML/CFT compliance yet. The Presidential decree to transfer the RSAA supervisory powers to Åland competent authority for real estate agents was yet to be passed as of the time of the on-site visit. (AML/CFT Act, Chapter 7, Section 1, subsection 1, paragraph 4).

AML/CFT supervisors do not have statutory powers to carry out the supervision of the implementation of the targeted financial sanctions obligations (see R. 6).

Criterion 28.3 – All categories of DNFBPs (except real estate agents in Åland: see c. 28.2 above) are subject to monitoring and supervision systems by relevant authorities or SRBs.

Criterion 28.4 –

(a) All supervisors have adequate powers to perform their functions and monitor compliance, which includes general powers to supervise, obtain information, carry out inspections, restrict activities of management, prohibit executions of decisions, and impose sanctions (AML/CFT Act, Chapter 7, Sections 1, 2, 3, 5, 6 and 7). There are some exceptions, however. The power to carry out routine on-site inspections is limited in case the premises where the supervised business is conducted are used for permanent residential purposes. Otherwise, inspections are only permitted when “there is justified cause to suspect that the obliged entity has ... seriously, repeatedly or systematically neglected or violated the Act” (see also criterion 27.2).

(b) The RSAA may refuse to register the agency where the person to be registered or, in the case of a legal person, a person holding a controlling interest (25%) or management position in the agency has been convicted of a criminal offence during the previous five years to a sentence of imprisonment or has been imposed fines

¹⁰⁴ Paf’s provision of gambling services is under the supervision of the Åland Lotteriinspektion (Regional Lotteries Act, Section 5a (1)). The authority of Lotteriinspektion does not yet include supervision of AML/CFT compliance. To meet constitutional muster, the AML/CFT supervision of gambling operators in Åland by the National Police Board must be transferred by Presidential decree to the Åland Lotteriinspektion (AML/CFT Act, Chapter 7, Section 1, subsection 1, item 2). This was not the case at the time of the on-site visit, as the Presidential Degree has only taken effect since July 1st 2018.

during the previous three years (Act on Real Estate Agencies and Housing Rental Agencies, Sections 5, 5a subsections 1(1) and 2 and section 8 subsection 1(3)).

Access to the profession of real estate agents in the Åland Islands is subject to registration with the Åland Government (Regional Decree on real estate agents, Section 3). Conditions for registration do not include measures to prevent criminals or their associates from being registered in Åland.

There are no measures in place to prevent criminals or their associates from being professionally accredited, or holding (or being the beneficial owner of) a significant or controlling interest, or holding a management function in other DNFBPs. In particular, there are no entry requirements or similar measures supervised by any competent authority with respect to lawyers, who are not members of the Bar Association.

(c) For breach of AML/CFT Act, RSAA is authorised to impose sanctions, such as administrative fines (up to EUR 10.000 for natural persons, and EUR 100.000 for legal persons), penalty payments (up to twice the gain resulting from the act or omission or EUR 1 million, whichever is higher) which may also be applied to a member of the management, public warnings (AML/CFT Act, Chapter 8, sections 1-4), as well as temporary restrictions of activities of DNFBP's management (AML/CFT Act, Chapter 7, section 5). These sanctions appear to be proportionate and dissuasive.

As far as the advocates are concerned, similar sanctions as set out above are imposed by the Regional State Administrative Agency on a reasoned proposal of the Finnish Bar Association (AML/CFT Act, Chapter 8, Section 1, subsection 6, Section 2, subsection 3, Section 3, subsection 4).

RSAA has power to cancel registration of a real estate agency (Act on Real Estate Agencies and Housing Rental Agencies, Section 19). RSAA has no power to revoke license or cancel registration of other supervised DNFBPs. In case of the real estate agencies in the Åland Islands, administrative or penal sanctions for failure to comply with the provisions of the Regional Decree on real estate agents are applicable (Sections 19 and 21). They include police warnings, business operations bans, and fines, unless a more severe punishment is applicable based on specific legal provisions. Applicable sanctions are therefore proportionate. The amount of fines is not specified in the law, and as such, it is impossible to judge whether these sanctions are dissuasive.

Since supervisors do not have statutory powers to carry out the supervision of the implementation of the targeted financial sanctions obligations (see c. 28.2) there is no sanction applicable.

Criterion 28.5 –

Mainland

When determining the scope and frequency of supervision, the supervisors (RSAA, National Police Board) and the Bar Association should have regard to (i) ML/TF risks concerning the supervised sector, supervised entities and their customers, products and services; (ii) the ML/TF risk assessments prepared by them (which in turn should be based on national and European-wide assessments); and (iii)

exemptions applicable to the activities of supervised entities (AML/CFT Act, Chapter 2, section 2). That seems to cover broadly the requirements of the c. 28.5. (a)-(b).

Åland Islands

(a) and **(b)** The Åland Lotteriinspektion is not a supervisory authority empowered by the AML/CFT Act (Chapter 7 Section 1) and therefore the requirements of the AML/CFT Act regarding the conduct of AML/CFT risk-based supervision are not applicable. There is no other requirement for the Åland Lotteriinspektion to conduct supervision on a risk-sensitive basis. The NPB was a nominal designated AML/CFT supervisor of PAF in Åland for one month; it did not exercise any supervisory powers over PAF under the AML/CFT Act.

Weighting and Conclusion: There are no specific fit-and-proper provisions applicable to the people in charge of the operational management of the casino or gambling operators. The authority of gambling and real estate supervisors in Åland Islands does not yet include supervision of AML/CFT compliance. AML/CFT supervisors do not have statutory powers to carry out the supervision of the implementation of the targeted financial sanctions obligations and there are no sanctions applicable. The power to carry out routine on-site inspections is limited in case the premises where the supervised business is conducted are used for permanent residential purposes. There are no measures in place to prevent criminals or their associates from being professionally accredited, or holding (or being the beneficial owner of) a significant or controlling interest, or holding a management function in most DNFBPs. RSAA has no power to revoke license or cancel registration of supervised DNFBPs other than real estate agencies.

Recommendation 28 is rated partially compliant.

Recommendation 29 – Financial Intelligence Units (FIU)

In its 3rd MER, Finland was rated largely compliant with these requirements (para. 215-257), mainly due to effectiveness concerns. The FATF Standards have been significantly strengthened in this area by imposing new requirements which focus on the FIU's strategic and operational analysis functions, and the FIU's powers to disseminate information upon request and request additional information from reporting entities.

Criterion 29.1 – Finland has an FIU which is part of the National Bureau of Investigation (Police). It acts as the national centre for receipt and analysis of suspicious transaction reports and other information relevant to ML, associated predicate offences and TF, as well as referring cases for criminal investigation (FIU Act, Section 2).

Criterion 29.2 –

(a) The FIU serves as the central agency for the receipt of STRs (AML/CFT Act, Chapter 4, section 1).

(b) The FIU serves as the central agency for the receipt of threshold-based reporting (AML/CFT Act, Chapter 4, Section 1, subsection 2).

Criterion 29.3 –

(a) The FIU has the authority to request and use any information from any reporting entity necessary to perform its functions (FIU Act, Section 4). The FIU has also competence to request information from any private sector entity in addition to reporting entities.

(b) The FIU has the authority to request any information necessary to perform its functions from any public body which includes Tax Authority, Bailiff (Enforcement) Authority, and Customs (FIU Act, Section 4). The FIU may also request information from SUPO (Finnish Security Intelligence Service).

Being a part of the national police force, the FIU has direct access to the following (Act on the Processing of personal data by the police, Section 13):

- Vehicle and Watercraft Registers
- Trade Register
- Border crossings of persons entering Finland with a visa
- Licence plate recognition (border crossings of vehicles)
- Visas granted by Finland to foreign nationalities
- Population Information System (family, address information).

The FIU has direct access to the criminal investigation database (Police, Customs, Border Guard), criminal intelligence database (Police, Border Guard), Schengen Information System (Act on the processing of personal data by the police, Chapter 2) and to Europol information system, database on MLA requests, as well as through request, Interpol information (Act on the processing of personal data by the police, Chapter 6).

Criterion 29.4 –

(a) The FIU conducts operational analysis by virtue of requirements to “analyse reports on suspicions of ML and TF” and other relevant information and “refer cases for criminal investigation” (FIU Act, Section 2).

(b) There is no legal requirement to conduct strategic analysis. However, the FIU does conduct strategic analysis in practice. In 2013-2017, the FIU has produced several pieces of strategic analysis.

Criterion 29.5 – The FIU is able to disseminate, spontaneously and upon request, “*information obtained*” for the purposes of “*preventing, detecting and investigating ML and TF, ... predicate offences ..., as well as referring cases for criminal investigation*” (FIU Act, Section 4, subsection 4). There are no restrictions with regard to the range of authorities that the information can be disclosed to. The scope of the disclosures is defined as the “*information obtained*” by the FIU (which includes information from STR reporting, the information requested from reporting and other entities, and information from databases).

The disseminations should be made via dedicated, secure and protected channels (Regulation on the classification and handling of secret information within the branch of government of the Ministry of the Interior, Section 3.7).

Criterion 29.6 –

(a) The information stored in the FIU database can only be accessed by the members of the FIU and can be disclosed only for the purposes of preventing, detecting and investigating ML and TF, predicate offences, as well as referring cases for criminal investigation (FIU Act, Section 3, subsection 4). There are requirements to ensure that localities and systems for processing personal data and other information may only be accessed by those who need the information for the performance of their tasks (Personal Data Act, Chapter 7, Act on the Processing of Personal Data by the Police, section 19b). In addition, the handling of classified information is regulated by the police internal rules, namely the Regulation on the classification and handling of secret information within the branch of government of the Ministry of the Interior.

(b) All FIU employees are subject to security clearances and training concerning the access to documents, confidentiality and professional secrecy (Act on Security Clearances, Section 19).

(c) The FIU is physically located in the premises of the National Bureau of the Investigation (NBI). Access to the building and also access to different parts in the building is controlled physically and electronically and restricted to a limited number of authorised personnel. FIU information is stored in electronic form in the FIU case management and analysis system which is protected by several security mechanisms in place to prevent unauthorized access. The servers are located in the secure environment, which has the strict security and access rules. The FIU database can only be accessed by the personnel of the FIU (Act on FIU, Section 3).

Criterion 29.7 –

Finnish FIU is operationally independent and autonomous.

(a) The Finnish FIU has 29 staff members and it has the authority to make autonomous decisions to analyse, request and disseminate information (FIU Act, Section 4). These decisions on requests can be taken at the level of “*a commanding police officer working at the Unit*”.

(b) The Finnish FIU has an explicit duty under law to cooperate with domestic competent authorities and foreign counterparts (FIU Act, Section 2), and it is authorised to engage independently with them on the exchange of information (FIU Act, Sections 4 and 5).

(c) The FIU is located within the National Bureau of Investigation (NBI), but it has distinct core functions which are stipulated in a separate FIU Act.

(d) The FIU is administratively and financially semi-independent. The head of the FIU is appointed by the Head of the NBI by open call procedure. All the open vacancies are also appointed by open call process organised by the NBI. These procedures are based on the Act on the Government Officials Chapter 3, section 6a. The FIU may refuse proposed persons. The Head of NBI has the power to relocate the FIU staff to other departments, but he also has the responsibility to ensure that the FIU has resources required to fulfil its statutory functions.

The NBI has decision-making power on the allocated resources and the annual budgetary issues. The Head of the FIU is competent to decide acquisitions of up to EUR 5,000 each (NBI Criminal Intelligence Division Rule of Procedures Chapter 5.4.3). Acquisitions above the EUR 5.000 threshold up to EUR 50.000 are decided by

the Head of the Intelligence Department and acquisitions above this by the Head of the NBI.

The Head of the Unit is also competent to decide on the operational international travel of the FIU personnel. The administrative personnel rules and guidance relating to all police administration are binding on FIU personnel as the personnel are acting as police officers.

Criterion 29.8 – The Finnish FIU is a member of Egmont group since 1998.

Weighting and Conclusion:

Recommendation 29 is rated compliant.

Recommendation 30 – Responsibilities of Law Enforcement and Investigative Authorities

In its 3rd MER, Finland was rated largely compliant with these requirements (para 266 to 301), because of insufficient attention being paid to pursuing ML and TF offences, and due to a lack of statistics that made difficult for assessors to evaluate the effectiveness of the system. This is not assessed as part of technical compliance under the *2013 Methodology*.

Criterion 30.1 – The Police, including local police departments and the National Bureau of Investigation (NBI), is a law enforcement authority for ML, associated offences, and TF offences (Police Act, Chapter 1, section 1 subsection 1). The prosecutor participates in the criminal investigation (Criminal Investigations Act, Chapter 1, Sections 1 and 2, Chapter 2, Section 1 (3)). The Customs is also a criminal investigation authority with equal powers compared to the Police. The investigative competence of the Customs is limited to customs offences prescribed in the Act on the Prevention of Crime by the Customs, Chapter 1, Section 2). The Border Guard is also involved in investigations (Criminal Investigations Act, Chapter 2, Section 1(2)) involving the production of financial benefit (proceeds of crime) to the extent that ML investigations should be pursued is limited.

Criterion 30.2 – Law enforcement investigators of predicate offences are authorised to pursue parallel financial investigations, regardless of where the predicate offence occurred (Criminal Investigations Act, Chapter 1, Sections 1 and 2, Chapter 3, Section 8).

Criterion 30.3 – The Police has the capacity to identify, trace, freeze and seize property that is or could become subject to confiscation, on a temporary basis, without waiting for a court decision (Coercive Measures Act, Chapter 6, section 3 (1)). Even though there is no obligation to act “expeditiously”, the Police has the possibility to act immediately, when freezing has to be done urgently in order to prevent assets from being moved (Criminal Investigation Act, Chapter 3, Section 11(1)(3); Coercive Measures Act, Chapter 6, Section 3(1)).

Criterion 30.4 – Although the majority of financial investigations (including ML and TF) are carried out by specialised police units, the FIU, which is also a police unit, has powers for pursuing financial investigations, which it uses in only very exceptional circumstances. It benefits from the same powers as the Police for its investigations since the Criminal Investigations Act is applied to the investigation of any criminal offences (Chapter 1, Sections 1 and 2, Chapter 2, Section 1). This

includes the same powers and competences to initiate freezing or seizing directly under the Police Act, the Criminal Investigations Act and the Coercive Measures Act.

Criterion 30.5 – There is no dedicated anti-corruption enforcement authority in Finland. The investigation bodies referred to in c. 30.1 are also competent to investigate ML/TF offences associated to corruption offences.

Weighting and conclusion –

Recommendation 30 is rated compliant.

Recommendation 31 – Powers of Law Enforcement and Investigative Authorities

In its 3rd MER, Finland was rated compliant with these requirements (para 302 to 301).

Criterion 31.1 –

(a) Competent authorities conducting investigations have powers to use compulsory measures for the production of records held by FIs, DNFBPs and other natural or legal persons. This includes the Police, including local police and NBI (Police Act, Chapter 4, Sections 2-4; Criminal Investigation Act and Coercive Measures Act) and the Customs (Act on the Processing of Personal Data by the Customs, Section 13) and Border Guard (Act on the Processing of Personal Data by the Border Guard, Sections 17-18).

(b) Competent authorities (Police, Customs and Border Guard) have powers to use compulsory measures for the search of persons and premises (Coercive Measures Act, Chapter 8, Sections 1 to 19 for searches of premises and from sections 30 to 33 for personal searches; Act on the Prevention of Crime by the Customs).

(c) Competent authorities have powers to use compulsory measures for taking witness statements (Criminal Investigation Act, Chapter 6, Section 1; Act on Combating Crime in Customs, Chapter 2, Section 1 and Coercive Measures Act, Chapter 1, Section 4).

(d) Competent authorities have powers to use compulsory measures for seizing and obtaining evidence (Coercive Measures Act, Chapter 7, Sections 1 and 7).

Criterion 31.2 – It is noted here that the relatively low threshold between the basic ML offence and the aggravated ML offence¹⁰⁵ is relatively low which limits the impact of the deficiencies listed below.

(a) The Police and Customs can use covert operations during the criminal investigation of certain serious offences specified in law, but only for aggravated ML and TF offences (Coercive Measures Act, Chapter 10, Sections 14-15). As regards the Customs, they can also apply these covert activities for aggravated ML and TF offences situations but under conditions set out in the relevant provisions of law (Act on Preventing Crime by Customs, Chapter 3, Section 11 and 12). The Border Guard can also apply these covert activities under the conditions set out in the relevant

¹⁰⁵ EUR 13 000 has been defined as the monetary threshold for the aggravated offence in the legislative preparatory works, but this is not a legal nor strict limit as the intentional manner, the complexity of the arrangements to conceal proceeds of crime also contribute to qualify an ML offence as aggravated.

provisions of law (Act on preventing crime by the Border Guard, Section 58). These provisions do not cover all associated predicate offences neither other type of ML offences.

(b) Competent authorities conducting investigations are able to intercept communications but only for aggravated ML and TF (as defined in Chapter 34a) in the Criminal Code), and not for other type of ML offences (Coercive Measures Act, Chapter 10, Section 3(2)(9) and (11)). The same applies for traffic data (Chapter 10, Section 6 (2) and (6)). In addition, criminal investigation authorities may conduct on-site interception in domestic premises in terrorist financing cases (chapter 10, section 17), and on-site interception outside of premises used as a permanent residence (Chapter 10, section 16), technical observation (chapter 10, section 19) in aggravated ML and all TF cases, and relevant predicate offences.

(c) Competent authorities conducting investigations, including Customs and Border Guards, are able to access computer systems if the suspected offence is ML or TF (Coercive Measure Act, Chapter 8, Section 21) and predicate offences (most severe punishment for the offence is imprisonment for at least 6 months or if the matter being investigated involves circumstance connected to the imposition of corporate fine).

(d) Competent authorities conducting investigations are able to use controlled delivery if there are grounds to suspect an offence for which the most severe punishment provided is imprisonment for at least 4 years (Coercive measures Act, Chapter 10, section 41). This implies that only aggravated ML and TF offences are concerned and not all associated predicate offences. For narcotics offences, other covert activities are available under Chapter 10, section 14, without restriction as to the level of sentence. The Border Guard and the Customs apply their own legislation to controlled delivery, in the situations and under the criteria set out in the relevant provisions of law (Act on Preventing Crime by the Border Guard, sections 37 and 61; Act on Preventing Crime by Customs, Chapter 3 section 42).

Criterion 31.3 –

(a) The mechanism to identify whether natural or legal persons hold or control accounts involves that the Police gets access – on request – to information held by both public authorities and private legal or natural persons. (Police Act, Chapter 2, Section 1, and Chapter 4, Sections 2(1) and 3(1) or FIU Act, Section 4). Enquiries must be done to each private entity separately. This mechanism does not ensure a timely identification of persons who hold or control accounts.

(b) Competent authorities have a process to identify assets without prior notification to the owner, as the head of investigation may prohibit a person present in the criminal investigation from revealing information to third parties if that may hamper clarification of the offence (Criminal Investigations Act, Chapter 11, Sections 5(1) and 6).

Criterion 31.4 – Competent authorities conducting investigations of ML, associated predicate offences and TF are able to ask for all relevant information held by the FIU. This is provided in the FIU Guidance and Form to Request Information from the FIU and to the FIU Guidance on Disclosure of Information to Foreign Countries.

Weighting and conclusion: Finland has some minor deficiencies as regards the range of investigative techniques that competent authorities can use for ML, associated predicate offences and TF. In particular, most of these techniques cannot be used for any types of ML offence or predicate offence, and some of them are not available to all the competent authorities.

Recommendation 31 is rated largely compliant.

Recommendation 32 – Cash Couriers

In its 3rd MER, Finland was rated partially compliant with these requirements. This was mainly due to the EU Regulation and relevant national legislation that did not cover the transfer of cash or bearer negotiable instruments between Finland and other EU Member States. In addition, as most measures were new at the time of the 2007 assessment, the effectiveness of the system could not be demonstrated, but this is not assessed as part of technical compliance under the *2013 Methodology*.

Criterion 32.1 – EU Regulation 1889/2005 obliges natural persons leaving or entering the EU to declare cash including bearer negotiable instruments (BNI) of a value of EUR 10 000 or more. The *Act on Controls of Cash Entering or Leaving the European Community 653/2007* supplements the EU Regulation and includes the EU definition for BNI. Customs can also stop and inspect postal and freight consignments (Customs Act, Chapter 3, Section 8). For internal EU traffic, Customs have the right to inspect the funds and other possessions carried by a person in order to detect a ML and TF offences.

Criterion 32.2 – A full and complete written declaration has to be made to Customs by all travellers entering or leaving the EU and carrying cash of a value of EUR 10 000 or more (EU Regulation 1889/2005, Art. 3.1; Cash Control Act, Sections 2 and 3). It is punishable to deliberately or through negligence neglect the obligation to declare or submit an incomplete or incorrect declaration (Act on Controls of Cash Entering or Leaving the European Community 653/2007, Section 9, i).

Criterion 32.3 – (N/A) Finland applies a declaration system.

Criterion 32.4 – There are a number of general measures, but no specific provisions that enable Customs to request and obtain further information on controls conducted, in order to determine whether import/export requirements are met (e.g. EU Regulation No 952/2013; Customs code (Art.5 (3), Art. 15 and Art. 46; Customs Act 304/216, Sections 8 and 102). Customs have also a general duty to ask questions to people who have breached their declaration obligations (Explanatory Memorandum (see Chapter 1) HE 153/2015 to the Parliament for the Customs Act and certain other related Acts, EU Handbook of Guidelines on Cash Controls).

Criterion 32.5 – Persons who make a false declaration are subject to fines applicable for a cash declaration violation, which range from 1 to 120 days fines (Cash Control Act, Section 9). The failure to declare a significant amount of cash or the intentional failure (when the money is hidden or when clearly false information are declared) can be considered factors that increase the number of day fines. Day fines are based on the taxable income of a person (Section 2 and 3), and the final amount is decided by the competent court (see c.24.13). This could affect the dissuasiveness of sanctions, as the minimum sanction could be EUR 6 for persons who do not have an official taxable income (see c.24.13).

Criterion 32.6 – Finnish Customs must communicate the declaration information to the FIU (Cash Control Act, Section 8).

Criterion 32.7 – There is co-ordination between Customs and the FIU on issues related to the implementation of R. 32 (see c. 32.6). Generally speaking, Police, Customs and the Border Guard have a law-based co-operation in crime prevention, detection, investigation and enforcement concerning them (PCB cooperation), with the key objective to prevent serious cross-border crime (Act on Cooperation between the Police, Customs and the Border Guard (11.9.2009/687) and Customs 639/2015, Section 17, paragraph 1, sub-paragraphs 5 and 6). Customs have also demonstrated cooperation through several national and international operations focused on illegal cash and assets transportation. In addition, law enforcement authorities (Police, Customs and Border Guard) utilize the same Data System for Police Matters (i.e. criminal complaints register) meaning they have access to the same register in which the cash declaration violations are registered.

Criterion 32.8 –

(a) The FIU can order Customs and Border Guard to seize funds discovered during a customs clearance measure or in connection with a border check or border control for a maximum of ten working days when such action is necessary for preventing, detecting and investigating ML and TF (FIU Act, Section 6, Subsection 2).

(b) Measures enabling competent authorities to detain cash are applicable, when there is a failure to declare, which includes cases where information provided is incorrect or incomplete (EU Regulation 1889/2005, art. 3 and 4 (2), Cash Control Act, section 6).

Criterion 32.9 – The declaration system allows for international co-operation and assistance, but limitations apply. Customs can decide to make the declaration information available to the competent authorities of other Member States, the European Commission and third countries (Cash Control Act, Section 8). The exchange of information with other EU authorities is organised by EU Regulation 515/97, which calls for the implementation of a rapid and effective system to share information between custom authorities at the EU level (EU Regulation 1889/2005, art. 6). Exchange of information with third countries takes place within the framework of mutual administrative assistance, upon request by the respective competent authorities. Customs can exchange information with third country counterparts if there is a bilateral agreement signed.

Regarding the specific situations referred to in a) to c), Finland indicates that cash declaration violations are recorded in the Customs Control Data File (TTJ) and the information is then available to EU Member States. Furthermore, in suspicious cases, it is possible to file a RIF (Risk Information Form) but no details are available.

Finland also indicates that information on customs control measures taken and the further action proposed, and identification information on summary penal orders issues or investigation requests or criminal reports filed on the basis of an inspection may be collected, recorded and otherwise processed in the Customs control information system (Section 5 of the Act on the Processing of Personal Data by Finnish Customs). The information will be deleted from the customs control data system at the end of the sixth calendar year following the saving of the information (Act on the Processing of Personal Data by Finnish Customs, section 21).

Criterion 32.10 – Customs applies general measures to ensure the confidentiality of the information collected through the declaration system (Act on the Openness of Government Activities, Section 24, Subsection 1, Act on the processing of personal data by the Customs 639/2015).

Criterion 32.11 –

(a) A person who does not fulfil his/her obligation to declare cash or who submits incorrect information (which includes the illicit physical cross border transportation of cash) commits a cash declaration violation and can be fined from 6 to 20 day fines (Cash Control Act, Section 9; Handbook of guidelines for cash controls). A person who is carrying out a physical cross-border transportation of currency or BNIs that are related to ML/TF or predicate offence may be subject to criminal sanctions (under the AML/CFT Act or other provisions of the Penal Code). The illicit physical transportation of cash may also be considered a ML offence (Criminal Code, chapter 32, sections 6-10) or a TF offence (Criminal Code, chapter 34a, sections 5 and 5a). Deficiencies identified in c.3.9 and c. 5.6 impact this sub-criterion).

(b) The competent authority has the right to detain (for 5 working days) and seize cash carried into or from the European Union, if the measure is necessary in order to find out whether, based on other legislation, there is cause to take measures concerning the cash (Cash Control Act, Section 6). If there is a suspicion of ML/TF or a predicate offence, Customs can contact the Police who can seize the cash in order to perform further investigation. Customs can also perform the criminal investigation in suspected ML offences, when they are related to customs offences (Customs Act, Section 2(1)(8)). Cash which has been illicitly transported across borders can be seized (Coercive Measures Act, Chapters 6 and 7). Deficiencies identified in R.4 impact this sub-criterion.

Weighting and conclusion: Finland has some minor deficiencies as regards international cooperation and assistance and sanctions to persons carrying out cross border transportations of currency or BNIs related to MF/TF offence or predicates offences.

Recommendation 32 is rated largely compliant.

Recommendation 33 – Statistics

In its 3rd MER, Finland was rated partially compliant with these requirements (para.800). The main deficiencies related to the lack of statistics maintained by some authorities, for ex. formal requests to/from supervisors, and the lack of comprehensiveness of other sets of statistics, for ex. ML/TF investigations and properties frozen, seized or confiscated.

Criterion 33.1 –

(a) The FIU tasks include keeping statistics, in particular on STRs received and disseminated (FIU Act, section 2, 6)). Those figures are available in the FIU annual report (see Tables 1.1 and 3, 2016 annual report).

(b) and **(c)** There are no specific provisions regarding statistics on ML/TF investigations, prosecutions and convictions and on property frozen, seized and confiscated. However, there are general provisions requiring national authorities to provide data on their activities and resources (Act on statistics, section 14). Courts

are required to enter their decisions or the conclusions of their decisions into the national information system, on the basis of which the Ministry of justice produces statistics (Act on the national information system of the court administration, section 6). There are similar obligations for enforcement authorities (Enforcement code, section 24). While appropriate statistics are maintained on ML/TF investigations, prosecutions and convictions, no comprehensive and reliable sets of statistics are available on property frozen, seized and confiscated in ML/TF related cases.

(d) The FIU is required to keep statistics on requests for information submitted, received, refused and complied with (FIU Act, section 2, 6), NBI internal rules for procedures). The Police maintains statistics on ML international information exchanged through the SIENA channel and MLA requests sent and received from non-EU countries. However, there is no other information available regarding MLA and other international requests related to ML/TF cases, to/from judicial authorities.

Weighting and conclusion:

Recommendation 33 is rated largely compliant.

Recommendation 34 – Guidance and feedback

In its 3rd MER, Finland was rated partially compliant with these requirements (para.475-481 and 485). The main deficiencies related to the lack of AML/CFT guidance provided by relevant authorities, especially to DNFBPs. The 2013 Exit from regular follow-up report noted that Finland has made progress with regard to all deficiencies identified and reached a level essentially equivalent to largely compliant.

Criterion 34.1 – The FIU Best Practices are comprehensive guidelines directed at all obliged entities, which cover various AML/CFT aspects based on the FIU expertise, and which are published by the FIU on its website. They need to be updated to reflect the amendments brought to the AML/CFT Act in 2017/18. The FIU website also provides specific guidelines on suspicious transaction reporting and includes a link to the electronic reporting system. The FIU also provides general feedback to reporting entities (ex. annual report with an analysis of STR reporting to the main reporting entities, 2016 and 2018 ML/TF risk indicators, typologies, trainings, seminars).

The financial supervisor, FIN-FSA, provides general guidance and information on AML/CFT compliance issues, including on suspicious transaction reporting (section 5.9 of standard 2.4 updated in 2015 on *Customer due diligence - Prevention of money laundering and terrorist financing*¹⁰⁶), and participates to training programmes.¹⁰⁷ It also interacts several times a year with financial trade bodies to discuss issues

¹⁰⁶ FIN-FSA standards are “a collection of subject-specific regulations and guidelines which both obliges and guides supervised entities and other financial market participants, indicates the quality level expected by the supervisor, sets out the supervisor’s key principles of good practice and provides justification for regulation”.

¹⁰⁷ www.fin-fsa.fi/en/Supervision/Money_laundering/Pages/Default.aspx and for STRs www.finanssivalvonta.fi/en/Supervision/Money_laundering/If_suspect/Pages/Default.aspx

relating to supervision and regulation. The RSAA, which is the body responsible for the supervision of some financial institutions and a number of DNFBP sectors (see c. 26.1 and 28.2, and Tables 1.1 and 1.2 in Chapter 1), published in 2015 general instructions regarding the prevention of ML and TF, including STRs,¹⁰⁸ directed at all parties under its supervision and in 2017, Guidelines on complying with the legislation to prevent TF.

Other supervisors (with the exception of the Finnish Patent and Registration Office) and the Bar association have developed general guidance for the implementation of and compliance with AML/CFT measures (with no specific focus on STR), and/or interact with supervised entities to provide general information.

Weighting and conclusion: General information and guidance is provided to all sectors. However not all supervisors, and especially DNFBP supervisors, have issued guidance on detecting and reporting suspicious transactions, which amounts to a moderate shortcoming.

Recommendation 34 is rated partially compliant.

Recommendation 35 – Sanctions

In its 3rd MER, Finland was rated partially compliant with these requirements (para 528), principally as money remitters and foreign exchange offices were only subject to criminal sanctions for violation of their AML/CFT obligations, the scope of regulatory authorities' ability to sanction natural persons was unclear and the Insurance supervisor had a relatively limited range of sanctions. The 2013 Exit from regular follow-up report noted that Finland had made progress with regard to most deficiencies identified and reached a level essentially equivalent to a largely compliant.

Criterion 35.1 – Sanctions available to supervisory authorities in case of a breach of AML/CFT obligations by obliged entities include administrative fines, penalty payments (for serious, repeated and systematic breaches), as well as public warnings. Clear criteria and maximum/minimum amounts are defined to determine proportionate sanctions, with distinctions made between financial and non-financial institutions and legal and natural persons (AML/CFT Act Chapter 8, Sections 1 to 5). There is a five-year time limitation concerning the right to impose administrative fines and public warnings sanctions, and a ten-year limitation for penalty payments (AML/CFT Act Chapter 8, Section 7). The 5-year limitation is a deficiency, given the supervision cycle applied by supervisory authorities.

There is also a limitation in the sanctions regime applicable, which weakens the proportionality of applicable sanctions to natural persons: when a breach can be punished both under the AML/CFT Act and the Criminal Code, supervisors have discretion to assess whether there is reason to report a failure to comply with AML/CFT obligation to the police as a potential criminal offence. If the supervisor decides to report the failure to the police, he would refrain from imposing a penalty

¹⁰⁸. www.avi.fi/documents/10191/2370358/K+General+instructions+2015/f611548f-bde3-4d1b-a116-095db4eff3a1.
General instructions and guidelines are available at www.avi.fi/sv/web/avi/tiedotteet-ja-ohjeet

payment, since in Finland, an action cannot be the basis for both criminal and administrative sanctions (*ne bis in idem* principle). If the police decides not to initiate a criminal investigation, the failure could then remain unpunished. However, this would not apply if criminal proceedings target a natural person and administrative proceedings (penalty payment) target the legal person (FI or DNFBP) (AML/CFT Act, Chapter 8, Section 3, subsection 3; Section 6, subsection 2).

Regarding violations of TFS TF obligations (R. 6), the Criminal Code provides sanctions (a fine or imprisonment for at most 2 years) for the violation of the Freezing Act, applicable to UNSCR 1373 only, and only for violations of the ban on providing, transferring or converting assets of designated persons and not for failure to freeze funds (Chapter 46, Section 1(2)). Violations of the Sanctions Act are also punished by a fine or imprisonment for at most 2 years (Criminal Code, Chapter 46, Section 1(1)). Supervisors do not have a statutory duty to supervise such obligations and therefore have no powers to apply administrative sanctions for failure to apply TFS (see R. 27 and 28).

Regarding sanctions applicable to NPOs, criminal sanctions are applicable in case funds are collected by unregistered NPOs and fines can be imposed when NPOs neglect to submit financial records, but there is no information available on applicable sanctions when NPOs fail to comply with their obligation to register (see c. 8.4. b).

Criterion 35.2 – The administrative fines and penalty payments applicable in case of a breach of AML/CFT obligations are applicable to natural persons (AML/CFT Act Chapter 8, Section 1, subsection 3, Section 4 subsection 3). Administrative sanctions can be imposed on executives of a legal person, and penalty payments are explicitly applicable to members of the management (AML/CFT Act Chapter 8, Section 3, subsection 5, see c. 35.1). In addition, supervisors can impose restrictions of activities of an obliged entity's senior management and directors for up to 5 years if he/she has demonstrated obvious incompetence or carelessness in the performance of duties and it is apparent that this may seriously jeopardise the achievement of the AML/CFT Act objectives (Chapter 7, section 5; FIN-FSA Act, Chapter 3, Section 28). However, in the case of lawyers, sanctions are only applicable to natural persons (lawyer or assistant) and not to law firms (AML/CFT Act, Chapter 8, Section 1, subsection 6; Section 2, subsection 3; Section 3, subsection 4).

Weighting and conclusion:

Recommendation 35 is rated partially compliant.

Recommendation 36 – International instruments

In its 3rd MER, Finland was rated partially compliant both for the international conventions and for UN Resolutions (para 714). The 2013 Exit from regular follow-up report noted that Finland had reached a level essentially equivalent to largely compliant. The main deficiency related to the implementation of Art. 18 of the International Convention for the Suppression of the Financing of Terrorism (TF Convention), in relation to ascertaining the identity of beneficial owners.

Criterion 36.1 – Finland has ratified the Vienna Convention, the Palermo Convention, the United Nations Convention against Corruption and the TF Convention.

Criterion 36.2 – Finland has broadly implemented the provisions of the Vienna Convention, the Palermo Convention, the United Nations Convention against Corruption and the International Convention for the Suppression of the Financing of Terrorism. However, the deficiencies identified with regard to the ML offence (R. 3) show that some specific provisions of the Vienna Convention (Art. 3), Palermo Convention (Art.6), Merida Convention (Art. 23) and the TF Convention (Art. 2) have not been fully implemented.

Weighting and conclusion: Finland has ratified the conventions but there are some deficiencies regarding the implementation of some of their provisions.

Recommendation 36 is rated largely compliant.

Recommendation 37 – Mutual legal assistance (MLA)

In its 3rd MER, Finland was rated largely compliant for these requirements (para. 725). The main technical deficiency related to the dual criminality requirement and the limitations of the ML/TF offences.

Criterion 37.1 – The Act on International Legal Assistance in Criminal Matters (ILACM Act) provides the legal basis for Finnish authorities to provide a wide range of mutual legal assistance in relation to ML, associated predicate offences and TF investigations, prosecutions and related proceedings¹⁰⁹. Finnish authorities may provide legal assistance to the authorities of another country directly on the basis of the ILACM Act regardless of whether there is a valid treaty with the country issuing the request. The requesting country is not required to provide reciprocal legal assistance to Finland. However, in individual cases, the Ministry of Justice may decide to refuse assistance, due to the absence of reciprocity from the requesting country (Section 16).

A request for legal assistance shall be executed “without delay” to the relevant authority (ILACM Act, Section 9). Assistance regarding European Investigation Orders (EIO) coming from counterparts from EU countries (except Denmark and Ireland) is governed by the Act on the implementation of EU Directive 2014/41 regarding the EIO in criminal matters (EIO Act). The provisions of the EIO Directive shall be complied with as law unless otherwise provided by the EIO Act (EIO Act, Section 1).¹¹⁰

Criterion 37.2 – There is an established official mechanism for MLA requests in Finland. Requests from foreign countries are made to the Ministry of Justice or directly to the authority competent to execute the request (ILACM Act, Section 4).

If a request has been sent to the Ministry of Justice, the Ministry forwards it, without delay, to the authority competent to execute the request, unless the execution of the

¹⁰⁹ The ILACM Act applies only to such legal assistance that is not governed by the Act on the Implementation of the EU Directive regarding the European Investigation Order in criminal matters (430/2017) (Section 1.3.) The ILACM Act is, however, applied in regard to the Republic of Ireland and the Kingdom of Denmark.

¹¹⁰ This legislation technique has been used in Finland for the transposition of Directives into national law. The technique has been accepted by the Constitutional Committee of the Finnish Parliament under certain conditions. The European Commission has not refused this technique in its assessments.

request falls within the competence of the Ministry of Justice. Under the EIO Directive, direct connections between the issuing and the executing authorities are applied (Article 7.1). Finland has designated the Ministry of Justice as the central authority to assist the competent authorities (Article 7.3, EIO Act, Section 4).

There is a request for timely prioritisation and execution of MLA requests (ILACM Act, Section 9) but no “clear process” is laid out as competent executing authorities have their own internal practices for the management of MLA requests. For EIOs, the relevant acts have to be carried out with the same celerity and priority as for a similar domestic case and, in any case, within the time limits provided (EIO Directive, art. 12). To monitor progress on requests, Finland indicates that authorities have case management systems in place, e.g. the police has a specific case management system for the processing of MLA requests and EIOs (KASI); there is a case management system in the Ministry of Justice (Central Authority) as of 1 May 2018 (VAHVA), which is common for all ministries.

Criterion 37.3 – Some restrictions apply to MLA with regard to reciprocity (see c. 37.1). In addition, discretionary grounds for MLA refusal include the fact that a decision has been issued in Finland or in a third state not to conduct a criminal investigation, (ILACM Act, Section 13.1)). This appears to be unreasonable or unduly restrictive condition. However, there is no obligation to refuse MLA in these cases, and this remains discretionary.

Criterion 37.4 –

(a) The ILACM Act does not include in its mandatory or discretionary grounds for refusal, offences involving fiscal matters (ILACM Act, Sections 12 and 13; EIO Directive, art. 11.3).

(b) The ILACM Act does not include bank secrecy in its mandatory or discretionary grounds for refusal (ILACM Act, Sections 12 and 13; EIO Directive, art. 11).

Criterion 37.5 – For international MLA requests, the confidentiality of the material provided by requesting countries is governed by Finnish legal provisions (ILACM Act, Sections 27 and 30.), as well as bilateral or multilateral agreements ratified by Finland. Regarding specifically cases where Finland is receiving MLA requests, there is no special clarifying provision, even though Finnish authorities indicate that Finnish law protects the secrecy of documents and other recordings, confidentiality, and parties’ and authorities’ right of access to information. For EIOs, confidentiality and secrecy measures similar to those applicable in Finland apply (EIO Act, Section 25). In addition, the conditions and procedures imposed by the competent authority of the other EU Member State concerning confidentiality, secrecy or restrictions on the use of the information shall be observed (EIO Directive, Article 19).

Criterion 37.6 – According to the ILACM Act a wide range of assistance can be given without the requirement of dual criminality. Only the use of coercive measures related to an MLA request is restricted by a dual criminality requirement, except for requests relating to an ML offence, where the suspect is an accomplice to the ML or predicate offence (ILACM Act, Section 15; EIO Directive, Article 10 and 11; EIO Act, Section 9).

Criterion 37.7 – The coercive measures may be used, if they would be allowed under Finnish law if the offence motivating the request was committed in Finland under

corresponding circumstances, and if the offence, had it been committed in Finland, would also have allowed the use of coercive measures (ILACM Act, Sections 15 and 23, EIO Directive, art. 10 and 11; EIO Act, Section 9)). This seems to *de facto* result in the need for the conduct underlying the offence to be criminalised in both countries, irrespective of the denomination or category.

Criterion 37.8 – The basis for the MLA system in Finland is that a request from a foreign country should be handled in the same way and with the use of the same means as if it were an investigation being carried out by a Finnish authority (ILACM Act, Section 9). The same principle is provided in the EIO Act (Section 8.1). This shall be observed in the MLA procedure for obtaining evidence and reports and hearing parties in criminal investigation, and service of a document should be conducted following the procedure that shall be followed in the service of corresponding documents under Finnish law (Sections 17 and 21). This would involve using the same powers and investigative techniques as those available for domestic investigations. The same applies for EIOs (EIO Act, art. 9.1). Direct connections of competent foreign authorities to Finnish counterparts are possible (see above). However, as laid out in c. 31.2, investigative techniques are not available for all types of ML offences and associated predicate offences.

Weighting and conclusion: The limited scope of the ML offence and the request for dual criminality remain MLA limitations. In addition, Finland does not have a clear process for the timely prioritisation and execution of MLA requests.

Recommendation 37 is rated largely compliant.

Recommendation 38 – Mutual legal assistance (MLA): freezing and confiscation

In its 3rd MER, Finland was rated largely compliant for these requirements (para. 742). The main technical deficiency related to the impossibility to confiscate property of corresponding value to the proceeds derived from ML.

Criterion 38.1 – There are provisions – with some minor limitations – providing that identifying, freezing, seizing and confiscating of property, proceeds, instrumentalities or property of correspondent value as those used in ML, predicate offences or TF at the request by foreign countries.

The Coercive measures Act regulates the basic material conditions under which freezing and seizing can be done. As concerns non-EU countries, Act on International Legal Assistance in Criminal Matters apply for freezing for the purpose of confiscation (Chapter 1, Section 1). The Act on Execution in the European Union of Orders Freezing Property or Evidence applies to requests for execution of a freezing order received from an EU Member State (Coercive Measures Act, Chapter 6, section 8).

The Coercive Measures Act includes measures to freeze “property” on the basis of a request from a foreign country for MLA (Chapter 6, Section 8) when “someone has, on the basis of a decision by a court of a foreign state in a criminal case, been ordered to forfeit an amount of money or if there are justified grounds to assume that someone shall, in a criminal case being.” This applies to all types of property targeted by the decision of the foreign court where the property belongs to a person who may be ordered, as a consequence of an offence, to forfeit an amount to the State, and the risk exists that said person will seek to evade payment of a fine, compensation,

restitution or forfeiture by hiding or destroying property, fleeing or in another comparable manner.

The Coercive Measures Act requires dual criminality for the enforcement of freezing orders (Section 3(1)). Offences punishable in another EU Member State by a custodial sentence of a maximum period of at least 3 years and part of a list provided could still be enforced, even though the criminal offence would not be punishable in Finland. This list includes terrorism-related offences and offences involving laundering of the proceeds of crime (Section 3(2)). The competent prosecutor has a duty to communicate “without delay” the freezing order enforcement decision to the district bailiff for enforcement (Section 9(1)). Deficiencies identified in R.3 as regards the scope of the ML offence have an impact on this criterion.

The Coercive Measures Act also provides seizure measures on the basis of a request from a foreign country for MLA (Chapter 7, Section 21). They apply to “*object, property, document or data*” which are undefined and therefore it is not possible to fully assess if a) to e) are targeted. Enforcement of a confiscation order pursuant to an MLA request is included in the Act on International Co-operation in the Enforcement of Certain Penal Sanctions (21/1987). The Act on the Implementation of the Provisions of a Legislative Nature of the Framework Decision on the Application of the Principle of Mutual Recognition to Confiscation Orders and on the Application of the Framework Decision (222/2008) applies to requests for executing a confiscation order received from an EU Member State. The normal international co-operation channels/ MLA requests would apply. Therefore, as seen in c.37.1 and c.37.2, there are some provisions for the timely execution of requests, but the deficiencies noted in R. 4 on confiscation would have an impact on this criterion.

Criterion 38.2 – The CC provides that confiscation may be ordered even if the perpetrator of the offence or act is not identified or if the perpetrator is not prosecuted or convicted, if there is sufficient proof for conviction is presented (Chapter 10, Section 1).

Criterion 38.3 –

(a) There are arrangements in place for coordinating seizure and confiscation actions with other countries. Finland is party to and applies different arrangements for coordinating seizure and confiscation on a Nordic level (Denmark, Norway, Iceland and Sweden, in addition to Finland), Baltic level, EU level and globally. The Asset Recovery Office (in the NBI) and the ARO network can also play a coordination role. Furthermore, Finland is party to the CARIN network. As far as coordinating investigations and the actions of judicial authorities in relation to seizure and confiscation actions, both EUROPOL and EUROJUST also provide coordination mechanisms.

(b) – There are legislative measures applicable to the management and disposition of property frozen, seized or confiscated (Coercive measures Act, Chapters 6 (Section 10) and 7 (Section 13); Enforcement Code (Chapters 6 and 8).

Criterion 38.4 – On demand from a foreign authority, the Ministry of Justice may decide that the assets, in full or in part or the confiscated object shall be surrendered to the foreign country (Act on International Co-operation in the Enforcement of Certain Penal Sanctions, Chapter 2, Section 14(2)).

Weighting and conclusion: There are minor deficiencies as regards the scope of property that can be subject to identification, freezing, seizing, and confiscation at the request of a foreign country.

Recommendation 38 is rated largely compliant.

Recommendation 39 – Extradition

In its 3rd MER, Finland was rated largely compliant with these requirements (para 754). The main deficiency related to limits to extraditions, linked to gaps in the ML offence (self-laundering, ML conspiracy, conspiracy to conduct aggravated ML) and TF offence (individual terrorist with no link to a specific terrorist act).

Criterion 39.1 –

(a) Dual criminality and at least a minimum penalty of one year of imprisonment are required for an offence to be extraditable (Extradition Act, Section 4). ML and TF offences are thus extraditable offences (see c. 5.6 and 7). At EU level, ML offences are part of those allowing extradition without verification of double criminality (EU Extradition Act, Section 3(2) 9)). There is no dual criminality requirement for extraditions between the Nordic countries (Act on Extradition between Finland and Other Nordic Countries (Nordic Extradition Act), Section 2). However, the limitation on the scope of the ML offence identified in R.3 has an impact on this criterion.

(b) Finland indicates that authorities have appropriate case management systems in place but this is not documented. There is no clear process for the timely execution of the extradition requests in the Extradition Act. The EU Extradition Act stipulates that the relevant court has to decide on the extradition within 3 days after the requested person has consented. In any case, the court must decide on the question of extradition within a period of 26 days after the requested person has been apprehended or found in Finland. If for a special reason the decision cannot be taken within the prescribed time limits, it has to be taken as soon as possible (Section 32). The Nordic Extradition Act also includes time limits (Section 29).

(c) Finland does not place the execution of extradition requests under unreasonable or unduly restrictive conditions.

Criterion 39.2 – Requests for extradition of Finnish citizens to a country other than an EU Member State or a Nordic country will not be granted (Extradition Act, Section 2). However, whenever Finland refuses extradition of a Finnish national who has committed ML in another country, Finland will have jurisdiction on the basis of Criminal Code, Section 6 (“Offence committed by a Finn”) and Finnish law would apply would therefore apply to an offence committed outside of Finland by a Finnish citizen. Under Finnish law, criminal investigation authorities are obliged to investigate the offence committed abroad in the same way as a “domestic” offence (this would include “undue delay”) and to submit the results of the investigation to the prosecutor for the consideration of further measures subject to the same restrictions as in a “domestic” case, if there is reason to believe that an offence has been committed (Criminal Investigation Act Chapter 3, section 3).

Criterion 39.3 – Extradition is granted, if the act referred to in the extradition request is an offence for which the most severe punishment under Finnish law is at least one year’s imprisonment or if the act, had it been committed in Finland under

corresponding circumstances, would be deemed such an offence (Extradition Act, Section 4; EU Extradition Act, Section 2(1)). This seems to *de facto* result in the need for the conduct underlying the offence to be criminalised in both countries, irrespective of the denomination or category.

Criterion 39.4 – Finland applies simplified extradition mechanisms with other EU and Nordic countries (ex. EU Council Framework Decision 2002/584/JHA on the European Arrest Warrant, EU Extradition Act Sections 3 (extradition without verification of double criminality), 5 (grounds for mandatory refusal), 6 (grounds for optional refusal), 13 (order of contacts), 14 (content and form of the request), 16 (apprehension), 32 (time limits), 41 (urgent nature of the consideration), 46 (time limits for execution) and 55 (order of contacts)).

Weighting and conclusion: There are limited processes for the timely execution of extradition requests including prioritisation where appropriate.

Recommendation 39 is rated largely compliant.

Recommendation 40 – Other forms of international cooperation

In its 3rd MER, Finland was rated largely compliant with these requirements (para 769). Statistics were not available to allow for sufficient evaluation of Finland’s investment in international cooperation, but this is an effectiveness issue not looked at as part of the TC analysis.

General principles

Criterion 40.1 – Finnish authorities are able to provide the widest range of international co-operation to EEA Member States. The information can be provided both spontaneously and upon request and most often through a single contact point. However, as outlined below, there are some minor deficiencies. Besides, there is no overall obligation to provide information “rapidly”. For non EEA Member States, Finland uses Memorandum of understanding (MoU), see below.

Criterion 40.2 –

(a) Most competent authorities have a legal basis to provide international cooperation:

- FIU (FIU Act, Section 2, subsection 4 and Section 5);
- Police (Act on the implementation and application of Council Framework Decision on simplifying the exchange of information and intelligence between law enforcement authorities of the Member States of the EU, Section 5; Act on the Processing of Personal Data by the Police, Chapter 6, Sections 29 (EEA counterparts) and 30 (non-EEA counterparts); Act on International Legal Assistance in Criminal Matters, for indirect cooperation (via the Ministry of Justice), section 3 subsection 2, paragraphs 2 and 3; for direct cooperation, section 5 subsection 1);
- Customs (Act on the implementation and application of Council Framework Decision on simplifying the exchange of information and intelligence between law enforcement authorities of the Member States of the EU, Section 5; 22 bilateral agreements signed with third countries, which allow cooperation and information exchange ; Act on International Legal

Assistance in Criminal Matters for indirect cooperation (via the Ministry of Justice), section 3 subsection 2, paragraphs 2 and 3; for direct cooperation, section 5 subsection 1);

- FIN-FSA (FIN-FSA Act, Section 3 subsection 3, 7) and 8); Sections 3a) and 50 and 54);
- Finnish Patent and Registration Office (Auditing Act, Chapter 9, Section 3).

There is no specific legal provision for the international cooperation of other supervisors. For the RSAA, if necessary, the generally applicable legislation could be applied, in particular the general data protection legislation (provisions on cross-border information exchange), and the legislation on the publicity of official documents.

(b) Competent authorities are not prevented from using the most efficient means possible for providing the widest range of assistance.

(c) Most competent authorities use secure gateways and mechanisms to transfer their requests:

- The FIU uses the FIU.net and Egmont Secure Web channels;
- The Police uses the Europol Secure Information Exchange Network (SIENA) system and bilateral police cooperation exchanges are encrypted;
- Customs uses secure gateways (Mutual Assistance Broker/OLAF; Risk Information Form (European Commission with EU Member States, and the SIENA system through Europol). Between World Customs Organisation member countries the CENcomm connexion is in place. For other counterparts, the electronic communication over encrypted networks is in use.
- FIN-FSA's secured email service is used for communicating confidential information with external parties (Deltagon Sec@GW solution). Between FIN-FSA and the ECB, a secured connection is also used, through automatically encrypted e-mails (TLS).

There is no information available on the secure gateways and mechanisms used by other supervisors.

(d) FIU's responses to requests for information shall be given without undue delay (FIU Act, Section 5, subsection 3).

The Police uses a single point of contact for international cooperation, and the Customs a central coordination unit. Both provide a 24/7 service. However, it is unclear how those mechanisms enable the Police and Customs to prioritise and execute timely international cooperation requests.

FIN-FSA has entered into several MoUs with international counterparts, some of which requiring that the exchange of information is provided on a timely basis. There is no information available on how other supervisors prioritise and execute timely international cooperation requests.

(e) Information provided by foreign counterparts to the FIU is appropriately protected under the Personal data Act, the FIU Act, the Act on the processing of personal data by the police and the Act on international legal assistance in criminal matters, as well as the Act on international data protection obligations. Information received by Customs and supervisors should be treated as secret official documents

(Act on the openness of government activities, Section 24 (2) and (3)) and are also protected under the Act on international data protection obligations. FIN-FSA does not apply a specific process for safeguarding information received from a foreign counterpart, although it may not disclose confidential information received from the supervisory or other authorities of another state or obtained in the course of inspections conducted in another state, without the express consent of the supervisory authority having provided the information or any other relevant supervisory authority of the foreign state in which the inspection was conducted (FIN-FSA Act, Section 71).

Criterion 40.3 – With the exception of joint investigative teams (see c. 40.19), competent authorities do not need bilateral or multilateral agreements to cooperate internationally. However, some authorities such as the FIU have signed MoUs with their counterparts.

Criterion 40.4 – When requested, the FIU and Customs submit feedback on the requested information. In general, deficient requests are referred back to the requesting authority to be supplemented. Similarly, feedback would be given in case the information received is inadequate or cannot be used. There is no information available for other authorities.

Criterion 40.5 – Finland does not prohibit or place unduly restrictive conditions to the exchange of information or assistance.

(a) Competent authorities do not refuse requests involving fiscal matters;

(b) Laws do not require FIs or DNFBPs to maintain secrecy or confidentiality (AML/CFT Act, Chapter 7, Section 2; FIU Act, Section 4);

(c) Disclosure of information may be refused by the FIU if preventing, detecting or investigating ML or TF or such predicate offences as were committed to gain the assets or proceeds of crime subject to ML or TF, or referring cases for criminal investigation might be impeded, or on other reasonable grounds (which refers to a fundamental obstacle such the protection of human rights) (FIU Act, Section 5). However, FIN-FSA may refuse to cooperate for specific reasons, including if the request concerns a person and a case for which legal proceedings or an administrative process is pending in Finland (FIN-FSA Act, section 53 2));

(d) The FIU cooperates with other FIUs whatever their nature or status. The same applies to FIN-FSA which would co-operate with foreign bodies entrusted with similar responsibilities (FIN-FSA Act, Section 71, subsection 7). There is no restriction for other authorities.

Criterion 40.6 – The information received by FIN-FSA from foreign financial supervisors can only be used for the discharge of supervisory duties, or for the purposes for which the consent was given (FIN-FSA Act, Section 71 Subsection 5). Similar provisions apply in the case of information provided to the FIU by a foreign counterpart (FIU Act, Section 5 subsection 2). No information is available on the existence of controls and safeguards to ensure that the exchanged information is used appropriately.

Regarding the Police information received from a foreign counterpart, the conditions set by this counterpart concerning secrecy, non-disclosure, restrictions on the use of the data, onward transfer of the data and returning of the supplied

material have to be complied with. However, the Finnish Police may use data supplied for purposes other than for which it was supplied, if the data is essential for, among other things, preventing or investigating an offence that may be punishable by imprisonment, which would be the case for ML or TF. In that case, there is no requirement to inform the foreign counterpart (Act on the Processing of Personal Data by the Police, Section 31).

There is no information available for other competent authorities.

Criterion 40.7 – FIN-FSA and the Police, including the FIU, are bound by confidentiality/secretcy obligations when exchanging information with foreign counterparts (FIN-FSA Act, Section 71; Act on the Processing of Personal Data by the Police, Sections 29, 30 and 31). There is no specific provision applicable by other competent authorities when exchanging information with foreign counterparts but the general principles on the restrictions of access to public documents would apply (Act on Openness of Government Activities, sections 10, 24, subsection 1, 2), 3, 4 and 9; 30)..

Criterion 40.8 – The FIU is able to conduct inquiries on behalf of foreign counterparts and exchange with foreign counterparts in a similar way as for domestic inquiries (FIU Act, Sections 2.4 and 5 subsection 1 to 3). The FIU of an EU Member State may be given the right to carry out indirect searches on the basis of a hit/no hit system in the Finnish FIU register, in order to determine if the register contains any data on a given search subject (FIU Act, Section 5 subsection 4). There is no similar mechanism applicable for requesting FIU from outside the EU. For the financial supervisor, see c. 40.15. There is no information available for other competent authorities.

Exchanges of information between FIUs

Criterion 40.9 – The FIU has an adequate legal basis for providing cooperation on ML, associate predicate offences and TF (FIU Act, Section 2, subsection 4 and Section 5).

Criterion 40.10 – When requested, the FIU submits feedback for the requested and disseminated information. It may also spontaneously give feedback but this is not the standard procedure. This is based on practice and there is no legal requirement to provide feedback.

Criterion 40.11 – (*Met*) **(a)** and **(b)** The FIU has the power to exchange all information to which it has direct or indirect access to through public authorities or private entities, upon justified request (FIU Act, Section 5, Subsection 3 and Section 4, Subsections 1 and 2).

Exchanges of information between financial supervisors

Criterion 40.12 – FIN-FSA has an appropriate legal basis for providing cooperation to foreign counterparts, consistent with the international standards for supervision (FIN-FSA Act, Section 3, subsection 3, 7) and 8), with a specific focus on EEA supervisory authorities (FIN-FSA Act, Sections 3a and 50). FIN-FSA cooperates with third countries, in the specific circumstances of Section 54. There is no clear legal basis for cross-border cooperation for the RSAA.

Criterion 40.13 – FIN-FSA can only disclose information that is necessary for the discharge of duties by the foreign authorities (FIN-FSA Act, Section 71). This would include, where relevant, information domestically available to them, including information held by financial institutions (Chapter 7, section 2 AML/CFT and the provisions of the FIN-FSA Act, see c. 27.3). There is no clear legal basis for cross-border cooperation for the RSAA.

Criterion 40.14 – (a), (b) and (c) The FIN-FSA Act requires FIN-FSA to submit to the foreign supervisory authorities all information in its possession necessary for the performance of group supervision (FIN-FSA Act, Section 52 subsection 1, Section 54, Section 65 and 65 a), Section 71, 12)). . There is no clear legal basis for cross-border cooperation for the RSAA.

Criterion 40.15 – The FIN-FSA Act allows the supervisory authority of EEA countries, upon prior information to FIN-FSA, to undertake an inspection or to obtain information from the Finnish branch of the financial entity supervised by this foreign EEA authority (Sections 60 and 63 to 65). This could include conducting inquiries. For non-EEA branches or non-EEA group-wide supervision, FIN-FSA has a right to disclose information to the relevant bodies (FIN-FSA Act, Section 71, subsection 1, 3 and 12). This provision could include information required for the conduct of inquiries. In addition, the FIN-FSA can request information from FIs under its supervision, which could be based on an inquiry from a third country (FIN-FSA Act, Section 18). There is no clear legal basis for the RSAA.

Criterion 40.16 – FIN-FSA has to receive the express consent of the foreign supervisory authority to disclose confidential information received (FIN-FSA Act, Section 71 subsection 5). This condition applies only to confidential information received. There is no clear legal basis for cross-border cooperation for the RSAA.

Exchanges of information between law enforcement authorities

Criterion 40.17 – The Police, Customs and Border Guards can exchange any data with foreign counterparts, provided that it is essential for preventing or investigating an offence which may be punishable by imprisonment (Act on the Processing of Personal Data by the Police, Sections 29 and 30 (2) 3), Act on the Processing of Personal Data by Customs, Chapter 6, Section 26, Act on the Processing of Personal Data by the Border Guard, Chapter 4, Sections 38 and 39).

Criterion 40.18 – The Police can use the powers available domestically to conduct inquiries and obtain information on behalf of their counterparts, based on the agreements concluded as part of the Interpol, Europol and Eurojust co-operation. In addition, all powers recognised to law enforcement authorities (Police, Customs and Border Guard) by the Criminal Investigations Act and the Coercive Measures Act (e.g. freezing, confiscation) would apply in the same way as for the investigation of national cases.

Criterion 40.19 – Finnish investigative authorities may enter into arrangements with competent authorities of other countries to establish joint investigative teams, for the purpose of criminal investigations. The request for a joint investigative team must be made through Mutual Legal Assistance (MLA) (Act on Joint Investigation Teams, Section 1).

Exchanges of information between non-counterparts

Criterion 40.20 – The FIU can request information to any other authority than counterpart, specifying the intended use of the information (FIU Act Section 5). FIN-FSA can cooperate with other supervisory authorities or other bodies or entities (FIN-FSA Act, Section 71). There is no information available for other authorities.

Weighting and conclusion: Most competent authorities, and in particular those whose operations or activities have a strong international dimension, have a wide range of powers to cooperate internationally. There are shortcomings but they remain minor in the overall context of Finland.

Recommendation 40 is rated largely compliant.

Summary of Technical Compliance – Key Deficiencies

Compliance with FATF Recommendations		
Recommendations	Rating	Factor(s) underlying the rating
1. Assessing risks & applying a risk-based approach	LC	<ul style="list-style-type: none"> All Finnish authorities have not comprehensively identified and assessed their ML/TF risks. The NRA is outdated, which limits the authorities' ability to allocate resources based on risks and implement appropriate AML/CFT measures. There is no exemption from SDD measures when there is a suspicion of ML/TF.
2. National cooperation and coordination	PC	<ul style="list-style-type: none"> The AML Action Plan is based on an outdated NRA, and there is no similar approach for TF. A number of authorities should be part of the FATF Steering group on a permanent basis.
3. Money laundering offences	LC	<ul style="list-style-type: none"> The definition of ML requires an intentional intent which is not fully consistent with the Vienna and Palermo Conventions The criminalisation of self-laundering which is limited to aggravated ML. Conspiracy is also limited to aggravated ML
4. Confiscation and provisional measures	LC	<ul style="list-style-type: none"> The absence of confiscation of corresponding value of property laundered for ML, aggravated ML, and negligent ML is a deficiency that has a specific impact in Finland as a significant part of proceeds of crime leave the country. This hinders the capacity of authorities to recover the assets.
5. Terrorist financing offence	LC	<ul style="list-style-type: none"> The TF offence for an individual terrorist still requires a link to be made with the use of funds to finance a specific terrorist offence. Sanctions for TF are not fully proportionate nor dissuasive.
6. Targeted financial sanctions related to terrorism & TF	LC	<ul style="list-style-type: none"> Finland has minor shortcomings, the main one being that the national mechanism for the implementation of UNSCR 1267/1989 and 1988 needs to be clarified.
7. Targeted financial sanctions related to proliferation	LC	<ul style="list-style-type: none"> There are still some delays in transposing the UN designations into EU law, which raises the question of whether the freezing action takes place without prior notice to the designated person/entity.
8. Non-profit organisations	PC	<ul style="list-style-type: none"> There is a limited identification of the subset of NPOs at risk of TF abuse and of the nature of threats. This has an impact on the scope and implementation of risk-based supervision and monitoring measures
9. Financial institution secrecy laws	C	
10. Customer due diligence	LC	<ul style="list-style-type: none"> There is no direct prohibition from keeping anonymous/fictitious names accounts (or similar business relationships) for financial institutions other than credit institutions as well as payment institutions; The requirement to identify beneficial owner does not extend to customers which are natural persons. There is no explicit requirement to verify legal person's identity through the address of the registered office or a principal place of business; There is no exemption from simplified due diligence measures when there is a suspicion of ML/TF
11. Record keeping	C	
12. Politically exposed persons	LC	<ul style="list-style-type: none"> There is no requirement to determine whether a beneficial owner of a customer is a PEP

Compliance with FATF Recommendations		
Recommendations	Rating	Factor(s) underlying the rating
13. Correspondent banking	PC	<ul style="list-style-type: none"> Correspondent banking requirements only apply to non-EEA countries.
14. Money or value transfer services	C	
15. New technologies	LC	<ul style="list-style-type: none"> The requirement to assess risks does not extend to situations when a financial institution is considering the development of the new product or service before the offering to customers; Finland has not assessed all of the risks it identified; Only financial institutions supervised by the FIN-FSA are required to assess the risks of a new product and service prior to their introduction Consumer credit providers, currency exchange providers, and other financial service providers supervised by RSAA are not required to implement mitigating measures.
16. Wire transfers	C	
17. Reliance on third parties	LC	<ul style="list-style-type: none"> The 3rd party reliance requirements with regard to parties established in non- EEA members do not cover CDD and record keeping; The level of country risk is only considered if the country is not an EEA-Member.
18. Internal controls and foreign branches and subsidiaries	LC	<ul style="list-style-type: none"> There is no requirement to apply appropriate additional measures to manage ML/TF risks, when the legislation of the relevant State does not permit compliance with the home country CDD procedures.
19. Higher-risk countries	PC	<ul style="list-style-type: none"> The enhanced measures are not applied based on the call by the FATF, but rather based on the EC Regulation which only applies to non-EU/EEA states; Finland cannot apply countermeasures when it is called upon by the FATF, or independently.
20. Reporting of suspicious transaction	C	
21. Tipping-off and confidentiality	C	
22. DNFBPs: Customer due diligence	LC	<ul style="list-style-type: none"> Same deficiencies as identified under Recommendation 10 (see above) apply also to DNFBPs. The requirement to carry out an ML/TF risk assessment does not extend to situations when a DNFBP is considering the development of the new product or service before the offering to customers; Finland has not assessed all of the risks it identified. Same deficiencies as identified under Recommendation 17 (see above) apply also to DNFBPs
23. DNFBPs: Other measures	LC	<ul style="list-style-type: none"> There are no requirements with regard to screening procedures to ensure high standards when hiring employees. These requirements only apply to the branches and subsidiaries located in non-EEA Member States, and it does not include the requirement to apply appropriate additional measures to manage ML/TF risks. Same deficiencies as identified under Recommendation 19 (see above) apply also to DNFBPs; There are no specific mechanisms in place to inform the supervised entities of countries included in the FATF public statements in Åland islands.
24. Transparency and beneficial ownership of legal persons	PC	<ul style="list-style-type: none"> Finland has not assessed ML/TF risks with regard to legal persons it identified;

Compliance with FATF Recommendations		
Recommendations	Rating	Factor(s) underlying the rating
		<ul style="list-style-type: none"> • There are no specific requirements with regard to the location where the information on the members of right of occupancy associations, associations and religious communities should be maintained; • Mortgage societies and European Economic Interest Groupings are not required to maintain the list of the members; • There are no requirements to update any changes to or keep the list of shareholders/partners/members or authorised signatories for savings banks, mortgage societies, insurance associations, right-of-occupancy associations, European Economic Interest Groupings, associations and religious communities up-to-date; • There are no requirements concerning availability of beneficial ownership of companies; • There is no general requirement to cooperate with the competent authorities. • When operations of a legal person are terminated, there is no requirement to keep basic and beneficial ownership information; • There is no explicit provision that the Tax Administration may call for beneficial ownership information of any legal person; • There are no legislative or administrative measures in place to convert bearer shares to nominal or ordinary shares; • There is no direct prohibition on nominee directors and shareholders; • The sanctions available are not always proportionate and dissuasive; • There is no legal requirement to monitor the quality of assistance received from other countries in response to requests for basic and beneficial ownership information or requests for assistance in locating beneficial owners residing abroad.
25. Transparency and beneficial ownership of legal arrangements	LC	<ul style="list-style-type: none"> • There are no specific provisions requiring trustees to disclose their status as trustees of a foreign express trust or any trust to FIs and DNFBPs.
26. Regulation and supervision of financial institutions	LC	<ul style="list-style-type: none"> • Companies providing certain financial services (e.g. non-consumer loans, financial leasing) are not subject to registration or licencing • There is no requirement with respect to banks to have meaningful mind and management located within Finland; • There are no specific fit-and-proper requirements for the managers and owners of insurance companies, local mutual insurance associations, a central securities depository and a central counterparty, as well as companies providing certain financial services (e.g. non-consumer loans, financial leasing)
27. Powers of supervisors	PC	<ul style="list-style-type: none"> • Supervisors do not have statutory powers to carry out the supervision of the implementation of the targeted financial sanctions obligations; • In the case financial institutions use residential premises for the conduct of business activities, the powers of the supervisors to conduct inspections is limited; • There are no sanctions applicable for violation of targeted financial sanctions obligations
28. Regulation and supervision of DNFBPs	PC	<ul style="list-style-type: none"> • There are no requirements to prevent criminal or their associates from being the board members of casino operators or persons in charge of the operational management; • There is no AML/CFT supervision of gambling operators and real estate agents in Åland islands;

Compliance with FATF Recommendations		
Recommendations	Rating	Factor(s) underlying the rating
		<ul style="list-style-type: none"> Supervisors do not have statutory powers to carry out the supervision of the implementation of the targeted financial sanctions obligations and there are no sanctions applicable; In the case DNFBPs use residential premises for the conduct of business activities, the powers of the supervisors to conduct inspections is limited; There are no measures in place to prevent criminals or their associates from being professionally accredited, or holding (or being the beneficial owner of) a significant or controlling interest, or holding a management function in DNFBPs other than mainland real estate agents; RSAA has no power to revoke license or cancel registration of supervised DNFBPs other than real estate agencies.
29. Financial intelligence units	C	
30. Responsibilities of law enforcement and investigative authorities	C	
31. Powers of law enforcement and investigative authorities	LC	<ul style="list-style-type: none"> The range of investigative techniques that competent authorities can use for ML, associated predicate offences and TF does not cover any types of ML offence or predicate offence, and some of them are not available to all the competent authorities.
32. Cash couriers	LC	<ul style="list-style-type: none"> There are a number of general measures, but no specific provisions that enable Customs to request and obtain further information on controls conducted, in order to determine whether import/export requirements are met. Sanctions and fines applicable for cash declaration violation are not fully dissuasive, as the minimum sanctions – based on the day fine system – could be very low for persons who do not have an official taxable income. The declaration system allows for international cooperation and assistance, but limitations apply.
33. Statistics	LC	<ul style="list-style-type: none"> No comprehensive and reliable sets of statistics are available on property frozen, seized and confiscated in ML/TF related cases, and there is no information available regarding MLA and other international requests related to ML/TF cases, to/from judicial authorities.
34. Guidance and feedback	PC	<ul style="list-style-type: none"> Not all supervisors have issued guidance on detecting and reporting suspicious transactions.
35. Sanctions	PC	<ul style="list-style-type: none"> There is a 5-year time limitation concerning the right for supervisors to impose administrative fines and public warnings, which is a deficiency given the supervisory cycle. There are only sanctions for the violation of the TFS TF obligations under UNSCR 1373, and no sanctions for failure to freeze funds. There is no information available on sanctions for NPOs' failure to comply with their registration's obligations. Lawyers' sanctions are only applicable to natural persons, and not to law firms.

Compliance with FATF Recommendations		
Recommendations	Rating	Factor(s) underlying the rating
36. International instruments	LC	<ul style="list-style-type: none"> Finland has ratified the conventions but there are some deficiencies regarding the implementation of some of their provisions. Some specific provisions of the Vienna Convention (Art. 3), Palermo Convention (Art.6), Merida Convention (Art. 23) and the TF Convention (Art. 2) have not been fully implemented.
37. Mutual legal assistance	LC	<ul style="list-style-type: none"> The limited scope of the ML offence and the request for dual criminality remain MLA limitations Finland does not have a clear process for the timely prioritisation and execution of MLA requests
38. Mutual legal assistance: freezing and confiscation	LC	<ul style="list-style-type: none"> There are no clear provisions that ensure that authorities can confiscate in response to requests by foreign countries the required elements in 38.1
39. Extradition	LC	<ul style="list-style-type: none"> There are limited processes for the timely execution of extradition requests including prioritisation where appropriate
40. International Cooperation	LC	<ul style="list-style-type: none"> There is no specific legal provision for the international cooperation of some supervisory bodies of DNFBPs and of one financial supervisor. However, given the characteristics of the supervised entities which mainly conduct domestic activities, the impact of these deficiencies are limited. There is no specific applicable provision, or no information available regarding the international cooperation powers of some authorities, in particular with regard to the use of secure gateways and mechanisms to share information with counterparts, the provision of feedback on request, the existence of controls and safeguards to ensure that the exchanged information is used appropriately, the conduct of inquiries on behalf of foreign counterparts, the exchange of information with non-counterparts. However, this applies to authorities who seldom have to cooperate with foreign counterparts or authorities, see above. FIN-FSA, one of the financial supervisor, may refuse to cooperate for specific reasons, including if the request concerns a person and a case for which legal proceedings or an administrative process is pending in Finland. The FIU does not have a legal requirement to provide feedback to foreign counterparts.

Glossary of Acronyms

AML/CFT	Anti-Money Laundering / Countering the Financing of Terrorism
BNI	Bearer Negotiable Instrument
CDD	Customer Due Diligence
CT	Counter Terrorism
CFT	Countering the Financing of Terrorism
DNFBP	Designated Non-Financial Businesses and Professions
DPRK	Democratic People's Republic of Korea
EC	European Community
ECB	European Central Bank
EDD	Enhanced Due Diligence
EEA	European Economic Area
EU	European Union
FI	Financial Institution
FIN-FSA	Finnish Financial Supervisory Authority
FIU	Financial Intelligence Unit
FTF	Foreign Terrorist Fighters
ISIL	Islamic State of Iraq and the Levant
JCPOA	Joint Comprehensive Plan of Action
LEA	Law Enforcement Authority
MFA	Ministry of Foreign Affairs
ML	Money Laundering
MLA	Mutual Legal Assistance
MoU	Memorandum of Understanding
NBI	National Bureau of Investigation (within National Police Board, NPB)
NGO	Non -Governmental Organisation
NPB	National Police Board
NPO	Non-Profit Organisation
NRA	National Risk Assessment
PF	Proliferation (of weapons of mass destruction) Financing
PRH	Finnish Patent and Registration Office
RBA	Risk-based approach
RSAA	Regional State Administrative Agency for Southern Finland
SDD	Simplified Due Diligence
STR	Suspicious Transaction Report
SUPO	Finnish Security Intelligence Service
TF	Terrorist Financing
TFS	Targeted Financial Sanctions
UN	United Nations
UNSCR	United Nations Security Council Resolution
VAT	Value-Added Tax



© FATF

www.fatf-gafi.org

April 2019

Anti-money laundering and counter-terrorist financing measures - Finland

Fourth Round Mutual Evaluation Report

In this report: a summary of the anti-money laundering (AML) / counter-terrorist financing (CTF) measures in place in Finland as at the time of the on-site visit from 23 May to 8 June 2018.

The report analyses the level of effectiveness of Finland's AML/CTF system, the level of compliance with the FATF 40 Recommendations and provides recommendations on how their AML/CFT system could be strengthened.