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

COUNCIL OF EUROPE
CONSEIL DE L'EUROPE

MONEYVAL(2022)6

Anti-money laundering and counter-terrorist financing measures

Liechtenstein

Fifth Round Mutual Evaluation Report

May 2022

The Committee of Experts on the Evaluation of Anti-Money Laundering Measures and the Financing of Terrorism - MONEYVAL is a permanent monitoring body of the Council of Europe entrusted with the task of assessing compliance with the principal international standards to counter money laundering and the financing of terrorism and the effectiveness of their implementation, as well as with the task of making recommendations to national authorities in respect of necessary improvements to their systems. Through a dynamic process of mutual evaluations, peer review and regular follow-up of its reports, MONEYVAL aims to improve the capacities of national authorities to fight money laundering and the financing of terrorism more effectively.

The fifth-round mutual evaluation report on Liechtenstein was adopted by the MONEYVAL Committee at its 63rd Plenary Session (Strasbourg, 16 – 20 May 2022).

Contents

EXECUTIVE SUMMARY

1. This report provides a summary of the anti-money laundering and combating financing of terrorism (AML/CFT) measures in place in Liechtenstein as at the date of the onsite visit (6-17 September 2021). It analyses the level of compliance with the Financial Action Task Force (FATF) 40 Recommendations and the level of effectiveness of Liechtenstein's AML/CFT system and provides recommendations on how the system could be strengthened.

Key Findings

a) ML/TF risks have been assessed in a frank and impartial way and, overall, the authorities have demonstrated a good broad and convergent understanding of core money laundering (ML)/terrorist financing (TF) risks. Whilst there is a scope for a more comprehensive understanding of risk in some particular areas, this only requires refinements to a well-established risk process. Some threats and important inherent risks have not been fully examined, which affects understanding of ML risk. These include an estimation of the extent of use of Liechtenstein's financial sector to launder the proceeds of tax offences committed abroad, and information on the types and location of non-bankable assets that are administered by trust and company service providers (TCSPs). Extensive use is made of data collected by the Financial Market Authority (FMA) to understand TF risk. Risks are addressed successfully by national AML/CFT policies and activities and support the application of enhanced and simplified customer due diligence measures (CDD). However, some exemptions are in place that are not supported by a country assessment of risk, including one that applies to investment funds, which is used extensively. Objectives and activities of the competent authorities are commensurate with risks and policies. Cooperation and coordination among stakeholders is effective.

b) Liechtenstein's Financial Intelligence Unit (FIU) constitutes an important source of financial intelligence, and its analytical reports are considered to be of a high quality by its primary users - prosecutors and law enforcement authorities (LEAs). Whilst the majority of ML investigations are triggered by requests for mutual legal assistance (MLA)/information received by foreign counterparts, the FIU's analyses are an inevitable part of any investigation/operational activity carried out by LEAs. Suspicious activity reports (SARs)/suspicious transactions reports (STRs) filed by persons subject to the Due Diligence Act (DDA) are generally commensurate with the landscape of prevalent proceeds-generating crimes in the country. However, they have rarely targeted some of the higher risk predicate offences, e.g., tax offences. As regards TF-related reporting, submission of only seven SARs/STRs might appear low, however the assessment team (AT) did not observe that persons subject to the DDA were not vigilant enough in exercising their duties in this regard. The FIU has so far produced several comprehensive strategic analysis reports - mostly based on trends and methods explored by the Egmont Group. Yet, the country would further benefit from strategic analysis in relation to TF, laundering of proceeds of foreign tax crimes, and on appropriateness of SAR/STR reporting in relation to these offences. The size of the

jurisdiction allows prompt information exchange and intensive consultation amongst the relevant authorities. Whilst the FIU has the necessary infrastructure in place, additional resources would be required in view of managing its growing workload.

c) Liechtenstein's legal and institutional framework enables effective investigation and prosecution of all types of ML. Whilst the FIU, LEAs and prosecution authorities have high awareness of a need to consistently pursue all ML-related activities, there is a lack of ML investigations/prosecutions targeting sophisticated ML schemes which potentially include complex legal structures established and managed in Liechtenstein. Risks and threats identified in the national risk assessment (NRA) mirror the typologies already observed in the country. Consequently, consistency between the types of ML activity being investigated and prosecuted with the country's threats and risk profile and national AML/CFT policies has been attained, with the exception of threats posed by tax crimes committed abroad. The judiciary has achieved convictions for all (three) types of ML cases: of the two types of ML, self-laundering of the proceeds of fraud committed abroad is still a prevailing typology and third-party laundering is encountered infrequently as are autonomous ML prosecutions. Sanctions imposed are not sufficiently dissuasive and proportionate. Liechtenstein introduced and has applied in practice criminal justice measures where, for justifiable reasons, a ML conviction cannot be secured. These measures include: (i) non-conviction-based confiscation; and (ii) criminalisation of failure to report a suspicious transaction by a person subject to the DDA.

d) Confiscation of the proceeds of crime is pursued as a policy objective in Liechtenstein. This has not only been confirmed through different strategic and policy documents but also through introduction of a comprehensive legal framework and continuous strengthening of the capacities of LEAs and prosecutors, both of which consider seizure and confiscation as a priority action when investigating any proceeds-generating offence(s). Financial investigations are routinely applied and communication between different authorities appears to be smooth and fruitful in each phase of seizure/confiscation proceedings. Liechtenstein has a framework treaty with Switzerland which stipulates that the execution of cross border controls is delegated to the Swiss Border Guard Corps. Communication between the Swiss Border Guard Corps and the National Police is intensive and smooth. The outcome of the authorities' actions, both in terms of assets seized and confiscated, is generally in line with the country's risk profile.

e) Being geographically located between Switzerland and Austria, Liechtenstein closely cooperates with both countries in combatting terrorism and TF. The absence of TF prosecutions in Liechtenstein is generally in line with the country's risk profile. One TF investigation was carried out, but it did not result in further proceedings as no evidence of TF was found. This notwithstanding, the features of this case confirmed that the competent authorities are equipped with skills and knowledge on how to detect collection, movement and use of funds for TF purposes. Since there have been no prosecutions/convictions for TF, no conclusion could be made on proportionality and dissuasiveness of sanctions applied. Whilst there is no specific counter-terrorism related strategy developed by the country, the initiatives taken by Liechtenstein in the

field of CFT show an appropriate degree of commitment, inter-agency cooperation and awareness by the competent authorities. Although some measures to disrupt TF are available to the competent authorities (such as expulsion of foreigners as per the Foreigners Act) none of these has yet been applied in lieu of proceedings with TF charges.

f) Liechtenstein has a sound legal framework which ensures automatic implementation of relevant United Nations (UN) Security Council (UNSC) Resolutions (UNSCR) on targeted financial sanctions (TFS) related to TF and proliferation financing (PF) into the national framework. Amendments introduced in 2020 and 2021 set the competent national authorities and relevant procedures, in particular with regard to supervision and designation/listing/de-listing, parts of which have been implemented recently. So far, there have not been any designations made at national or UN level, which is consistent with the country's risk profile. Persons subject to the DDA demonstrated a generally good understanding of PF TFS-related obligations, while banks and large TCSPs demonstrated advanced practical knowledge in this regard. Understanding of most persons subject to the DDA in relation to identifying persons indirectly controlling or owning funds involved in transactions is limited to checking existing lists, whilst the majority of persons subject to the DDA (apart from banks and TCSPs) do not distinguish between TF- and PF-related TFS. So far, no assets have been frozen. PF TFS-related supervision has recently been introduced. While the FMA has already conducted some on-site inspections, this has not been done by the Chamber of Lawyers.

g) NPO risk analysis aimed at identifying the subset of non-profit organisations (NPOs) falling under the FATF definition and has resulted in the identification of 52 NPOs which might be exposed to high TF risk. Monitoring/supervision over foundations and establishments is carried out by several institutions: the FMA, Foundation Supervisory Authority (STIFA) and the Fiscal Authority. The NPO Risk Report was a trigger for additional oversight measures regarding those NPOs identified as high-risk. NPOs met onsite demonstrated a proper awareness of the Risk Report and of the risks they might be exposed to. This cannot be attributed to NPOs that are associations. The association met onsite was not aware of the obligations vis-a-vis CFT measures and the ways associations could be misused for TF.

h) Understanding of ML/TF risks and obligations is now generally good in the private sector. Banks and large TCSPs demonstrated the best understanding of ML/TF risks, linked to private banking and wealth management, and have implemented sophisticated measures to mitigate risk. In general, mitigating measures are now effectively applied and are commensurate with risk, though less attention was given to establishing and corroborating source of wealth (SoW) and source of funds (SoF) and to the possible illicit uses of "shell" companies until more recently. In general, CDD (including enhanced measures) and record-keeping obligations are now being diligently applied. Reporting obligations have been met only to a limited extent and there has been less reporting than expected in respect of tax offences. Many persons subject to the DDA have never filed a SAR/STR, e.g., some TCSPs and asset managers,

and some banks and TCSPs have been reported to the Office of the Public Prosecutor (OPP) for failing to make reports. Generally, good controls and procedures are in place.

i) Controls implemented by supervisors are effective at preventing criminals from holding or being the beneficial owner (BO) of a significant interest or holding a management function. Positive steps have been taken by the FMA to improve its knowledge of ML/FT risks, including introduction of a specific supervisory risk model, and the FMA is considered to have a good understanding of risk. The FMA supervisory approach has been subject to a significant overhaul and greater use is now made of FMA inspections to conduct reviews of compliance with AML/CFT requirements. Direct FMA supervisory activity of entities that it assesses as presenting a high-risk or medium-high risk (predominantly TCSPs and investment funds) is not sufficient and resource constraints are a concern. In particular, the FMA is insufficiently equipped to deal with high risk and medium-high risk TCSPs. There has been a welcome move towards the use of focussed and thematic inspections, though there remains a need also for some more general supervisory activity to test compliance with the full range of preventive measures at all levels of risk. The use of monetary fines by the FMA has increased notably since 2019 but it is not possible to conclude that effective, proportionate, or dissuasive sanctions have been applied. Overall, the FMA continues to mostly use remedial supervisory measures to deal with breaches, and enforcement action against the TCSP sector is less than expected by the AT. Supervision by the Chamber of Lawyers is comparatively rudimentary but given the risk and size of the regulated sector, this is not a major concern.

j) The authorities have a good broad understanding of the risk that legal persons (and legal arrangements) may be used to launder the proceeds of crime. There is a less granular, documented understanding in respect of TF. A range of effective measures are in place to prevent misuse, including an obligation placed on legal persons that are predominately non-trading and wealth management structures (around 80% of legal persons) to appoint a "qualified member" (a TCSP) to sit on the governing body. Basic and BO information on legal persons and legal arrangements is available from registers maintained by the Office of Justice and directly from the private sector and there have been no difficulties accessing information in a timely manner. Basic information held by these sources is generally accurate and up to date, but it has not been demonstrated that this is the case also for BO information. At the time of the onsite visit, the Office of Justice had yet to start monitoring the completeness and plausibility of information held on the BO register and had placed reliance on qualified members to submit accurate information on a timely basis. However, the AT considers that there has been insufficient FMA supervisory oversight of the performance of CDD activities by such members. Also, BO information held by the private sector – which updates information based on risk – will not necessarily be up to date.

k) International cooperation constitutes an important part of Liechtenstein's AML/CFT system in view of the predominantly foreign nature of predicate crimes to ML. The country has a comprehensive legal and institutional framework to perform international cooperation. Competent authorities demonstrated effective cooperation in providing and seeking information, both through the use of formal and informal

channels, with a range of foreign jurisdictions. Some issues in relation to dual criminality requirements regarding tax evasion and obligation to hear an entitled party before rendering evidence to a foreign jurisdiction, could have an impact on effective cooperation. Several measures aimed at diminishing these risks have been implemented in recent years, thus minimising the risks posed by these legislative provisions.

Risks and General Situation

2. As an international financial centre (IFC), Liechtenstein's primary money ML threats stem from non-resident customers that may seek to transfer criminal proceeds that were generated abroad or use Liechtenstein financial intermediaries to facilitate their illicit activities. In this regard, economic crime (in particular fraud, embezzlement, fraudulent bankruptcy, and tax offences) and corruption are the most relevant predicate offences. The inherent risks for the financial centre result, in particular, from its international clientele and the services/products offered in the field of wealth management. All types of financial products and services that wealthy non-resident clients may seek are offered in Liechtenstein, including establishment and administration of legal persons and legal arrangements, bank accounts, trading in securities, insurance policies, virtual asset (VA) services etc. These could make the country an attractive location for layering criminal proceeds.

3. Liechtenstein has not experienced any terrorist attacks to date and the likelihood that it will become a target of terrorism is low. No terrorist organisations are operating or present in Liechtenstein and no parts of its population are sympathetic to terrorist causes. The threat of funds being used for terrorism in Liechtenstein is, therefore, low. Still, the risk that Liechtenstein may be misused for TF purposes is determined to be medium as funds may be moved through its financial system. As an IFC, services and products offered in Liechtenstein could potentially be used to finance terrorism abroad.

Overall Level of Compliance and Effectiveness

4. Liechtenstein has taken steps since its last evaluation to remedy the deficiencies identified during that process – the jurisdiction strengthened its legal and regulatory framework and conducted its first comprehensive NRA (covering the period from 2013 to 2015), which was then updated by its second iteration - finalised in July 2020.

5. In most respects, the elements of an effective AML/CFT system are in place, but the practical application of the existing framework has still to be improved in some areas to reach a substantial level of compliance. These improvements should, *inter alia*, include better understanding of the ML threats associated with the current tax regime; investigations/prosecutions of complex ML schemes which potentially include legal structures established and managed in Liechtenstein; increased supervisory activity for entities the FMA assesses as presenting a high-risk or medium-high risk; and a better understanding of reporting by persons subject to the DDA, etc.

6. In terms of technical compliance, the legal framework has been enhanced in many aspects, nevertheless, some issues remain, including measures applied with regard to new technology – VA and virtual assets service providers (VASPs) (R.15); regulation and supervision of designated non-financial businesses and professions (DNFBPs) (R.28) and sanctions for failing to comply with AML/CFT requirements (R.35).

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

7. Risks have been assessed in a frank and impartial way and, overall, the authorities have demonstrated a good broad and convergent understanding of core ML/TF risks. Whilst there is a

scope for a more comprehensive understanding of risk in some particular areas, this only requires refinements to a well-established risk assessment process.

8. Even though the risk of misuse of Liechtenstein's financial sector to launder the proceeds of tax offences committed abroad has been recognised, the extent of the threat has not been estimated. Two other ML threats have not been fully examined, these being: (i) the extent to which prominent global offences that have a transnational element may be laundered through the financial system in Liechtenstein; and (ii) understanding of transactional links to countries presenting a higher ML risk.

9. Some important inherent ML risks have not been considered which affect understanding of risk: (i) whilst the FMA now holds valuable information about TCSPs, this does not include data on the types and location of non-bankable assets that are administered by TCSPs - often held through complex structures; (ii) information is not held on the profile of customers of banks that subscribe for units in non-private investment funds; and (iii) there has been limited analysis of the use of cash.

10. Recent changes to Article (Art.) 165 of the Criminal Code (CC) - to include tax savings as asset components subject to ML - have largely curtailed use in the private sector of shell companies, which is conscious of the higher risk of such companies being used to make transactions now criminalised under the CC. However, understanding of how residual risk has changed in this area is rather limited.

11. Extensive use is made of data collected by the FMA to understand TF risk. Whilst the analysis and consequent understanding of transactional links to countries presenting a higher TF risk is insufficient, this is considered to have only a minor effect on risk understanding.

12. ML/TF risks, as acknowledged and analysed in national risk assessments, are addressed successfully by national AML/CFT policies and activities. The country's action plan does not include any explicit action to examine and estimate the extent of use of Liechtenstein's financial sector to launder the proceeds of tax offences committed abroad.

13. Cases triggering the application of enhanced CDD (EDD) and simplified measures are consistent with risks identified in the NRA. Some exemptions from the application of preventive measures are in place that are not supported by a risk assessment at country level, including one that applies to investment funds, which is used extensively.

14. Objectives and activities of the competent authorities are commensurate with risks identified in the NRA and policies. Cooperation and coordination among stakeholders is effective and constitute one of the strengths of Liechtenstein's system.

15. Based on efforts taken to share results, the private sector demonstrated a high level of awareness on NRA findings.

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

16. Liechtenstein's LEAs and prosecutors have access to and in practice make systematic use of a wide variety of sources of financial intelligence and other relevant information when investigating ML and predicate offences, tracing assets and identifying criminal money flows. Parallel financial investigation is an integral part of investigations of proceeds-generating crimes.

17. Whilst the majority of ML investigations are triggered by requests for MLA/information received by foreign counterparts, the FIU's analyses are an inevitable part of any investigation/ operational activity carried out by LEAs.

18. As regards SARs/STRs filed with the FIU, during the period under review a number of initiatives have taken place which resulted in an overall increase of the number of reports filed. Although the FIU expressed a general satisfaction with the quality of SARs/STRs received, some areas still warrant improvements, including the following: (i) although SARs/STRs filed by persons subject to the DDA are generally commensurate with the landscape of prevalent proceeds-generating crimes in the country, they have rarely targeted some of the higher risk predicate offences, e.g., tax offences; (ii) the increase in the overall number of SARs/STRs in recent years did not trigger a tangible difference in the number of FIU disseminations to LEAs; and (iii) the tendency of reactive or non-reporting, which was prevalent before 2018, can still be observed, although to a lesser extent.

19. Whilst the FIU has so far produced several comprehensive strategic analysis products, the AT has identified a need for further analysis or review of the appropriateness of SARs/STRs filed on: (i) laundering of foreign tax offence proceeds; and (ii) TF, taking into account transactions with TF-related high-risk jurisdictions. In addition, TF-related typologies, as well as red flags/indicators to support reporting suspicion of handling the proceeds of foreign tax offences would be an asset.

20. Liechtenstein's legal and institutional framework enables effective investigation and prosecution of all types of ML. The FIU, law enforcement and prosecution authorities have high awareness of a need to consistently pursue and investigate all ML-related activities. The OPP and the National Police regularly investigate financial elements of predicate offences and develop parallel financial investigations, the aim of which is twofold: (i) to identify proceeds of crime; and (ii) to identify the way these proceeds were laundered or attempted to be laundered through Liechtenstein financial institutions (FIs), DNFBPs or VASPs. Given that the vast majority of predicate offences have been committed abroad, ML investigations are mostly triggered by incoming MLA requests. Consequently, analysis of financial flows are essential and inevitable parts of any ML investigation carried out in Liechtenstein. This being said, and taking into account the context of an IFC, a lack of ML investigations/prosecutions targeting sophisticated ML schemes which potentially include complex legal structures established and managed in Liechtenstein has also been observed.

21. Risks and threats identified in the NRA mirror the typologies already observed in the country. Therefore, consistency between the types of ML activity being investigated and prosecuted with the country's threats and risk profile and national AML/CFT policies has been attained, with the exception of threats posed by tax crimes committed abroad. This type of criminality has never been subject to an ML prosecution in Liechtenstein. In addition, tax evasion is not an ML predicate offence which hampers the authorities' efforts to further investigate ML in relation to this offence when committed abroad. Whilst the judiciary has achieved convictions for all (three) types of ML cases: of the two types of ML, self-laundering of the proceeds of fraud committed abroad is still a prevailing typology and third-party laundering is encountered infrequently as are autonomous ML prosecutions. Sanctions imposed by Liechtenstein courts for ML offences are not proportionate and dissuasive.

22. Confiscation of the proceeds of crime is pursued as a policy objective. Introduction of a comprehensive legal framework and continuous strengthening of the capacities of LEAs and prosecutors to detect, seize/freeze and confiscate assets further confirm this statement. Competent authorities routinely carry out financial investigations parallel to any proceeds-generating crime investigation. They have managed to establish strong inter-institutional cooperation which works well throughout each phase of the seizure/confiscation proceedings. Judicial authorities are also vigilant and aware that proceeds may dissipate instantly and thus consider a grounded suspicion as sufficient to approve freezing orders (both for proceeds and instrumentalities of crime) over the course of a criminal investigation. Both conviction and non-conviction-based confiscation, including the confiscation of equivalent value, are frequently applied in practice. The amounts seized/frozen and confiscated are considerable. Although the amount of confiscated assets is still inferior to the sums seized/frozen, this mostly results from delays in receiving responses to MLA requests sent abroad. Furthermore, the authorities actively seek and provide assistance from/to their foreign counterparts when seeking/tracing proceeds of crime. The outcome of the authorities' actions, both in terms of assets seized and confiscated, is generally in line with the country's risk profile.

23. Liechtenstein has a framework treaty with Switzerland which stipulates that the execution of cross border controls is delegated to the Swiss Border Guard Corps. Statistics and discussions held with the Swiss Border Guard Corps revealed certain weaknesses in the system. However, the AT observed that communication between the Swiss Border Guard Corps and the National Police is intensive and smooth. Any infringement identified by the Swiss Border Guard Corps is immediately notified to the National Police.

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

24. There have been no TF prosecutions/convictions in Liechtenstein so far. The country has never received an MLA request from foreign counterparts in relation to terrorism or TF. The national TF risk assessment concluded that the risk of TF in Liechtenstein is medium. The absence of TF prosecution is generally in line with the country's risk profile. One TF investigation was carried out, but it did not result in further proceedings as no evidence of TF was found. This notwithstanding, the features of this case and actions undertaken by the competent authorities confirmed that they are equipped with skills and knowledge on how to detect collection, movement and use of funds for TF purposes.

25. Since there have been no prosecutions/convictions for TF, no conclusion could be made on proportionality and dissuasiveness of sanctions applied. On the other hand, sanctions, as envisaged by the CC for the TF offence, appear proportionate and dissuasive. There is no specific counter-terrorism related strategy developed by the country. However, the country has developed a TF Strategy, the main goals of which aim to develop the ability to prevent/suppress TF. Other initiatives undertaken by Liechtenstein in the CFT field show an appropriate degree of commitment, inter-agency cooperation and awareness by the competent authorities. Measures to disrupt TF are available to competent authorities (such as expulsion of foreigners as per the Foreigners Act), however none of these has yet been applied in lieu of proceedings with TF charges.

26. Liechtenstein's legal framework ensures automatic implementation of UN TFS related to TF/PF into the national framework. The country has recently further amended its legislation in

line with FATF Recommendations covering TF/PF TFS-related supervision, procedures for designation, listing and delisting. Liechtenstein has not identified any individuals or entities or proposed any designations under UNSCRs 1267/1989 or 1988 which is consistent with the TF risk profile of the country. Nor have domestic procedures in relation to UNSCR 1373 been tested in practice due to the absence of such cases.

27. Persons subject to the DDA demonstrated at least a generally good understanding of PF TFS-related obligations, while banks and large TCSPs demonstrated advanced practical knowledge in this regard. Smaller DNFBPs explained that they would mostly rely on banks as regards identification and subsequent freezing/reporting. Understanding of most persons subject to the DDA in relation to identifying persons indirectly controlling or owning funds involved in transactions is limited to checking lists. In addition, the Terrorism Ordinance does not provide for the obligation to freeze funds or other assets of persons and entities acting on behalf of, or at the direction of, designated persons or entities. As for the understanding on PF TFS, most persons subject to the DDA did not differentiate between TF and PF related TFS. So far, no UNSCR TF/PF TFS-related funds have been frozen.

28. Since 30 January 2020, supervisory authorities have been entrusted with authority to monitor compliance with the special obligations of persons subject to the DDA.

29. Monitoring/supervision of the NPO sector is conducted by several authorities, including STIFA and the Fiscal Authority, as well as the FMA as regards the supervision (as TCSPs) of qualified members of the governing body of NPOs. The supervisory activities conducted by the competent authorities cover the whole range of activities provided under the Interpretative Note to FATF Recommendation 8 (INR.8) as regards monitoring/supervision exercised over foundations and establishments. These activities were applied to all common-benefit foundations and establishments in an undifferentiated manner until the adoption of the NPO Risk Report, such that a risk-based approach, including a focus on TF aspects, was not implemented. Based on the NPO risk analysis conducted by the competent national authorities, 52 NPOs were identified as falling under the FATF definition and represent a high risk for TF. Based on the results of the NPO Risk Report, a number of risk-based initiatives were implemented in relation to these NPOs, including bilateral supervisory meetings and enhanced scrutiny by the FMA towards the qualified members of those NPOs. As for associations, these are currently subject to fiscal monitoring, although STIFA has started supervisory meetings with ones identified as high-risk based on the NPO Risk Report.

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

30. Understanding of ML/TF risks and obligations is now generally good among covered FIs, DNFPBs and VASPs. This was not the case for all the period under review. Amongst FIs, banks demonstrated the most sophisticated level of understanding of ML/TF risks (linked to private banking and wealth management and use of cash) and obligations. Amongst DNFBPs, TCSPs and casinos have the best understanding of risks and obligations (especially large TCSPs). The understanding of large VASPs was at the same level as large TCSPs.

31. In general, mitigating measures are now effectively applied and are commensurate with risk. This was not the case for all the period under review, e.g., less attention was given to establishing and corroborating SoW and SoF and to the possible illicit uses of “shell” companies. Banks and large TCSPs have implemented sophisticated measures to mitigate ML/TF risks.

Measures in place in other sectors are less robust but still satisfactory. Non-private investment funds widely apply an exemption that means that they are not required to identify and verify the identity of underlying investors but often do not have sufficient information available to adequately assess ML/TF risks.

32. In general, CDD and record-keeping obligations are being diligently applied. However, weaknesses have been identified during the period under review in respect of information held on SoF and SoW, with improvements noted following the strengthening of supervisory measures in 2019, and with customer profiling in the VASP sector. Record-keeping measures have been applied in line with R.11 by all sectors.

33. Generally, enhanced measures have been applied appropriately for: (i) PEPs; (ii) new technologies; (iii) wire transfers; (iv) TFS relating to TF; and (v) higher-risk countries identified by the FATF. Whilst FIs do not offer correspondent relationships, except for foreign subsidiaries, VASPs have relationships with similar characteristics. The effectiveness of measures regarding wire transfers and TFS have been hindered in the VASP sector, as the travel rule is not fully implemented in practice.

34. During much of the period under review, reporting obligations were met only to a limited extent. Whilst there has been a significant increase in reporting since 2019, there has been less reporting than expected by the AT in respect of tax offences. Many persons subject to the DDA have never filed a SAR/STR, e.g., some TCSPs and asset managers, and some banks and TCSPs have been reported by the FMA to the OPP for failing to make reports. Late reporting has also been observed in the TCSP and VASP sectors. Some smaller non-bank FIs and DNFBPs were unable to elaborate on typologies that could give rise to a SAR/STR. Internal policies/procedures and training are in place to prevent tipping-off.

35. FIs, DNFBPs and VASPs have generally good controls and procedures. AML/CFT compliance functions are properly structured and resourced and involve regular internal audits and training programmes.

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

36. Controls implemented by supervisors, including those applied on an ongoing basis, are effective at preventing criminals from holding or being the BO of a significant interest or holding a management function. These controls have successfully picked up a small number of cases of criminal involvement at pre- and post-licensing stages.

37. Positive steps have been taken by the FMA to improve its knowledge of ML/FT risks, including introduction of a specific supervisory risk model. Accordingly, the FMA is considered to have a good understanding of risk.

38. The FMA supervisory approach has been subject to a significant overhaul and greater use is now made of FMA inspections to conduct reviews of compliance with AML/CFT requirements. There is now also much greater FMA input into, and oversight of, commissioned inspections (conducted by auditors).

39. Direct FMA supervisory activity of entities that it assesses as presenting a high-risk or medium-high risk (predominantly TCSPs and investment funds) is not sufficient and resource constraints are a concern. The FMA is insufficiently equipped to deal with high risk and medium-

high risk TCSPs and has only been able to perform a marginal number of random checks on medium or medium-low risk institutions. Since 2019, there has been a welcome move towards the use of focussed and thematic inspections, though there remains a need also for some more general supervisory activity to test compliance with the full range of preventive measures at all levels of risk.

40. There has been a notable increase in the imposition of monetary fines since 2019. However, it is not possible to conclude that effective, proportionate, or dissuasive sanctions have been applied by the FMA. Overall, the FMA continues to mostly use remedial supervisory measures to deal with breaches and the number and level of monetary fines imposed during the period under review has been low. In particular, enforcement action against the TCSP sector is less than expected by the AT.

41. Supervisors promote a clear understanding of AML/CFT obligations and risks but have not clearly demonstrated that their actions have had an effect on compliance.

42. Supervision by the Chamber of Lawyers is comparatively rudimentary but given the risk and size of the regulated sector, this is not a major concern.

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

43. Detailed information is available publicly on the creation and types of legal persons and arrangements found in Liechtenstein. The authorities have a good broad understanding of the risk that legal persons (and legal arrangements) may be used to launder the proceeds of crime. There is less granular, documented understanding in respect of the risk of TF.

44. The authorities rely on a range of measures to prevent the misuse of legal persons and legal arrangements, including an obligation placed on legal persons that are predominately non-trading and wealth management structures (around 80% of legal persons) to appoint a qualified member to sit on the governing body. These measures are effective in helping to prevent misuse.

45. Basic and BO information on legal persons and legal arrangements is available from two sources: (i) registers maintained by the Office of Justice; and (ii) directly from the private sector. In practice, whilst BO information has been obtained by competent authorities through the BO register, those authorities also seek BO information directly from the private sector (including qualified members of legal persons), and law enforcement also from legal persons and legal arrangements. There have been no obstacles or difficulties accessing basic or BO information in a timely manner.

46. The AT considers that basic information held by these sources is generally accurate and up to date. A BO register has been in place since August 2019 and, with few exceptions, it holds adequate BO information on legal persons and legal arrangements. At the time of the onsite visit, the Office of Justice had yet to start monitoring the completeness and plausibility of information held on the register, and, instead, reliance was placed on qualified members of legal persons to submit accurate information to it on a timely basis. While the results of supervisory activity do not indicate particular issues in compliance with BO obligations, the AT considers that there has been insufficient FMA oversight of the performance of CDD activities by qualified members. This alternative to proactive oversight by the Office of Justice is therefore not considered to be sufficiently effective in demonstrating that BO information held in the register is accurate and up to date.

47. These shortcomings would not matter, or matter less, if combined access to information held in the BO register and BO information held by the private sector cumulatively ensured the availability of adequate, accurate and current information. However, BO information held by the private sector – which updates information based on risk – will not necessarily be up to date.

48. Sanctions taken in respect of failures to comply with basic information requirements are considered to be effective, proportionate, and dissuasive. However, administrative fines applied for failing to provide BO information to the Office of Justice are not.

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

49. Given the predominantly foreign nature of predicate offences to ML, international cooperation plays an important role in the country's overall AML/CFT framework. Liechtenstein has, in general, provided constructive and timely MLA and extradition across the range of international co-operation requests. Based on feedback from the global network, the authorities provide good quality cooperation to a large extent both in terms of MLA requests and other forms of cooperation.

50. Some issues were identified by the AT which could have an impact on the overall effectiveness of cooperation, these being dual criminality in relation to foreign tax evasion and the right by an entitled party to be heard before the court (and thus indirectly informed of an on-going investigatory action) prior to the execution of any MLA. Efforts have been made by the country to diminish these risks through: (i) provision of administrative assistance on foreign tax offences; and (ii) introduction of legislative changes to the MLA Act, which now gives the possibility to transmit relevant objects, documents, and data to the requesting authority and to postpone the right of the entitled party to be heard before the court up until the end of the investigation by the requesting party, thus minimising the risk of tipping-off.

Priority Actions

- Liechtenstein should conduct additional studies to examine and estimate the extent of ML threats associated with tax offences committed abroad. In line with the country's action plan, it should continue to improve its understanding of ML/TF threats presented by transactional links to countries presenting a higher ML risk. Follow-up action should be taken as necessary.
- Liechtenstein should consider collecting the following additional information in order to support its analyses of inherent risk: (i) types and location of non-bankable assets that are administered by TCSPs (e.g., foreign operational subsidiaries, high value goods and real estate); (ii) profiles of underlying investors in investment funds that benefit from CDD exemptions; and (iii) use of cash and prepaid cards, e.g. economic sectors presenting greater exposure and reasons, recurrent use of cash above certain thresholds, use of ATMs in countries that neighbour conflict zones, and trends. Follow-up action should be taken as necessary.
- The authorities should carry out further review/analysis with regard to: (i) SAR/STR reporting on high-risk predicates, i.e., laundering of foreign tax offences proceeds; and (ii) TF-related SAR/STR reporting taking into account transactions with TF-related high-risk

jurisdictions. Both reviews/analyses should be reviewed periodically, possibly through the public-private partnership platform.

- To support reporting obligations, the FIU should provide more granular sectoral guidance (especially for non-bank FIs and DNFPBs) and training on sector specific ML/TF methods trends and typologies, including major risks identified in the NRA.
- Liechtenstein authorities should ensure that the OPP, investigative judges, the National Police and the FIU effectively target complex, large-scale ML, including cases involving funds deriving from high-risk predicates committed abroad (corruption, tax crimes, trafficking in narcotic drugs, etc.) which are then layered through Liechtenstein FIs, DNFBPs or VASPs.
- Competent authorities should continue to prioritise investigations related to the financial component of predicate offences and improve their understanding of typologies related to the main risks the jurisdiction is facing.
- In order to further expedite all forms of international cooperation, Liechtenstein should introduce written procedures/guidance on the exact modus operandi to be followed by competent authorities when receiving MLAs related to fiscal matters (regardless if in a concrete case the dual criminality principle applies). Responses to the requesting state should outline the scope of information/administrative assistance that can be obtained from the Fiscal Authority. The authorities should also consider developing a standard template form for responding to these MLA requests.
- The FMA should review its targets for the frequency of supervisory activity of entities that it assesses as presenting a high-risk or medium-high risk (predominantly TCSPs and funds). When doing so, it should also consider the use of offsite supervision to ensure that a full range of AML/CFT obligations continues to be adequately assessed across all sectors.
- Liechtenstein should increase the number of staff that are available to the FMA to deal with high risk and medium-high risk TCSPs and investment funds and conduct more frequent random reviews of other risk categories.
- The FMA should make more extensive use of monetary fines particularly in those sectors identified as presenting a higher risk, in addition to requiring remediation of shortcomings.
- Competent authorities should invest further efforts to introduce and enforce risk-based monitoring/supervision for all NPOs representing a high-risk for TF (as identified by the NPO Risk Report), including associations.

Effectiveness & Technical Compliance Ratings

Effectiveness Ratings[1]

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
SE	SE	ME	ME	ME	SE
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**	
ME	SE	SE	ME	ME	

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	C	LC	C	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	LC	C	LC	LC	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**
LC	C	PC	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**
LC	LC	LC	LC	LC	LC
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	LC	PC	LC	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**
C	LC	LC	C	PC	C
R.37 – Mutual legal assistance	**R.38 – Mutual legal assistance: freezing and confiscation**	**R.39 – Extradition**	**R.40 – Other forms of international cooperation**		
LC	C	C	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 6 to 17 September 2021.

The evaluation was conducted by an AT consisting of:

- Ms Francesca Picardi, Senior Officer, Financial Security Committee, Department of the Treasury, Ministry of Economy and Finance, Italy (law enforcement/financial expert);
- Ms Laura Aus, Financial Sanctions Expert, Estonian Financial Intelligence Unit (legal expert);
- Ms Zaruhi Avakimyan, Coordinator, AML/CFT Team, Risk Assessment Center, Supervision Division of the Central Bank, Armenia (law enforcement expert);
- Mr Hamish Armstrong, Chief Advisor, Jersey Financial Services Commission, Crown Dependency of Jersey (financial expert);
- Mr Irakli Kalandadze, Head of Money Laundering, Inspection and Supervision Department National Bank of Georgia (financial expert); and
- Mr Marcus Schmitt, Senior Prosecutor, Public Prosecutor's Office for Combatting Economic Crimes and Corruption, Austria (legal expert).

The AT was supported by the MONEYVAL Secretariat:

- Mr Lado Lalicic, Head of Unit;
- Mr Andrew Le Brun, Deputy Executive Secretary; and
- Ms Ani GOYUNYAN, Administrator.

The report was reviewed by Ms Lia Umans, MONEYVAL Scientific Expert, Mr Mark Benson (Isle of Man) and the FATF Secretariat.

Liechtenstein previously underwent a mutual evaluation in 2014, conducted by the International Monetary Fund according to the 2004 FATF Methodology. The 2014 evaluation and 2018 exit follow-up report have been published and are available at https://www.coe.int/en/web/moneyval/jurisdictions/liechtenstein.

That mutual evaluation concluded that the country was compliant with eight Recommendations; largely compliant with 30 Recommendations; and partially compliant with 11 Recommendations. No Recommendation was rated non-compliant. Liechtenstein was rated compliant or largely compliant with ten out of 16 Core and Key Recommendations.

Following the adoption of the 4th Round mutual evaluation report (MER), Liechtenstein was placed under the regular follow–up procedure. In December 2018, Liechtenstein exited the follow–up process on the basis that it had reached a satisfactory level of compliance with Core and Key Recommendations in line with Rule 13, para. 4 of MONEVAL's Rules of Procedure.

1. ML/TF RISKS AND CONTEXT

1. The Principality of Liechtenstein (Liechtenstein) is situated between Switzerland and Austria in the centre of the Alpine arc. With a total area of 160 km^2, it is the fourth smallest country in Europe. Liechtenstein has a total of 38 747 inhabitants (December 2019). A third of the population are foreign nationals, mainly from Switzerland, Austria, and Germany.

2. Liechtenstein has a constitutional hereditary monarchy. The power of the state is embodied in the reigning Prince and the people and is exercised by both parties under the constitution. A five-member Government is nominated by the Parliament and appointed by the Prince for four years. The Government is the highest executive body in Liechtenstein and is organised as a Collegial Government, which is constituted by the Prime Minister and four Ministers. This Collegial Government is responsible to the highest legislative body, the Parliament, as well as to the Prince as Head of State. The 25 Members of Parliament, called Landtag, are elected by the people for four years in universal, direct, and secret elections.

3. Liechtenstein takes an active part in international affairs, having close relations with neighbouring countries of Switzerland and Austria and membership of numerous international organisations. The country joined the European Free Trade Association as a full member in 1991 and has been a member of the European Economic Area (EEA) since 1995 and the Schengen agreement since 2011. Through the EEA, the 27 Member States of the European Union (EU) and the three EEA EFTA States are integrated into the Internal Market. The EEA Agreement guarantees equal rights and obligations within the Internal Market for individuals and economic operators in the EEA. It provides for the inclusion of EU legislation covering four freedoms – the free movement of goods, services, persons, and capital - throughout the 30 EEA States. Inter alia, Liechtenstein is also a member of the Council of Europe (since 1978), the UN (since 1990), and the Organisation for Security and Co-operation in Europe (since 1975).

4. In 1923 Liechtenstein entered into a customs and monetary union with Switzerland, which remains in place to this day. The latter entails that the Swiss National Bank is responsible for the entire "Swiss franc (CHF) currency area" (Switzerland and Liechtenstein), exercising associated monetary and currency policy functions.

1.1. ML/TF Risks and Scoping of Higher Risk Issues

1.1.1. Overview of ML/TF Risks

5. As an international financial centre (IFC), Liechtenstein's primary money laundering (ML) threats stem from non-resident customers that may seek to: (i) transfer criminal proceeds that were generated abroad to, or through, Liechtenstein; or (ii) use trust and company service providers (TCSPs) to facilitate their illicit activities. In this regard, economic crime (in particular fraud, embezzlement, fraudulent bankruptcy, and tax offences) and corruption are the most relevant predicate offences. The inherent risks for the financial centre result, in particular, from its international clientele and the services/products offered in the field of wealth management. Liechtenstein financial intermediaries often handle mandates of considerable complexity that require a high degree of know-how. This offer is particularly important for very wealthy clients due to the value and type of assets involved and cross-border nature of business.

6. The financial centre is able to offer all types of financial products and services that wealthy non-resident clients may seek - establishment of legal entities, administration of structures, bank accounts, trading in securities, insurance policies, VA services etc. These could make the country an attractive location for layering criminal proceeds. In Liechtenstein, these different services are often provided by a single service provider, e.g., groups that consist of asset managers, TCSPs and law offices. These products and services can be used to transfer illicit funds to destination countries involved in the integration process.

7. Domestic threats are minimal as Liechtenstein has a comparatively low crime profile, with a low volume of criminality and proceeds generating crimes.

8. Liechtenstein has not experienced any terrorist attacks to date and the likelihood that it will become a target of terrorism is low. No terrorist organisations are operating or present in Liechtenstein and no parts of its population are sympathetic to terrorist causes. The threat of funds being used for terrorism in Liechtenstein is, therefore, low. Still, the risk that Liechtenstein is being misused for terrorist financing (TF) purposes is determined to be medium as funds may be moved through its financial system. As an IFC, services and products offered in Liechtenstein could potentially be used to finance terrorism abroad.

9. Residual ML and TF risks are explained under Chapter 2.

1.1.2. Country's Risk Assessment & Scoping of Higher Risk Issues

10. In 2016, Liechtenstein conducted its first comprehensive national risk assessment (NRA) (covering the period from 2013 to 2015) based on the World Bank methodology. An executive summary covering the results and accompanying explanations was published in 2018 after consultation with the private sector. Risk-based actions were subsequently identified, and an Action Plan was adopted at the end of 2018 and has since been updated regularly.

11. Starting in 2019, the NRA was updated, and its second iteration finalised by July 2020 - based on data from 2016 to 2018. The assessment is divided into the following three parts, which together are referred to as NRA II: (i) NRA of Money Laundering Risks of the Liechtenstein Financial Centre (NRA – ML); (ii) NRA of Terrorist Financing of the Principality of Liechtenstein (NRA – TF); and (iii) NRA on Money Laundering and Terrorist Financing Risks of the Liechtenstein Financial Centre with regard to Virtual Assets (NRA – VA).

12. NRA II was developed using a holistic approach involving all the authorities and offices represented on the Working Group on the Prevention of Money Laundering, Terrorist Financing and Proliferation (PROTEGE WG), as well as the Ministry of General Government Affairs and Finance. In particular, the following authorities and agencies played a key role in the creation of NRA II: (i) the Financial Market Authority; (ii) the OPP; (iii) the Office of Justice; (iv) the Fiscal Authority; (v) the National Police; (vi) the Court of Justice; (vii) the FIU; and (viii) the Office for Foreign Affairs.

13. During the process, information, including statistical data, was provided by stakeholders across the public and private sectors. Information was analysed and assessed at workshops involving relevant authorities and meetings of the PROTEGE WG. NRA II takes into account both quantitative and qualitative information, including: (i) key ML/TF threats – based on cases investigated, convictions obtained, information from the FIU (e.g., SARs/STRs), assets restrained

in relation to specific crimes, and numbers of international requests for assistance; (ii) key ML/TF vulnerabilities of financial products/activities, including the level of AML/CFT controls (e.g., availability and enforcement of criminal sanctions, effectiveness of supervision procedures and practices, effectiveness of suspicious activity monitoring and reporting etc.); and (iii) experts' views as well as feedback from public and private sector stakeholders.

14. Some non-financial sectors (including lawyers, accountants (including auditors and auditing companies), dealers in goods and real estate agents) which were assessed as presenting medium-low/low ML residual risk in NRA I were not re-analysed in NRA II based on these earlier risk assessments and observation of no changes. Risks presented in these sectors by forming and administering legal persons and legal arrangements were covered by NRA II (as part of an assessment of TCSPs).

15. An update of the NRA VA was made in August 2021. The first risk analysis was carried out at a point within the transition period for the newly introduced registration requirement for VASPs. As a result, there was little data available on the few VASPs active at the time and the assessment largely focused on general risks associated with VAs.

16. In addition to NRA II, the following have been conducted: (i) an analysis of the risks associated with Liechtenstein legal persons and legal arrangements in relation to ML (May 2020); and (ii) an analysis of the TF risks of non-profit organisations (NPOs) (May 2020) - to identify those legal entities that fall within the functional FATF definition and are most at risk of abuse for TF purposes. Findings in these two additional analyses were used to define concrete measures in the Action Plan.

17. Whilst there is scope for a more comprehensive understanding of ML/TF risk in some particular areas, this requires refinements to a well-established risk process and the authorities have demonstrated a good broad and convergent understanding of core ML/TF risks in the financial, TCSP, casino and VASP sectors. The country has also demonstrated a sufficiently broad understanding of risks in other sectors too. Chapter 2 sets out some areas where the AT considers that risks may not be fully examined and understood.

18. In advance of the on-site visit, the AT identified several areas requiring increased focus in the evaluation through an analysis of information provided by the authorities and by consulting various open sources.

19. Since Liechtenstein's main risk stems from *external threats*, the AT considered the awareness of resulting risks by the private sector and extent of the public-private partnership in mitigating these risks, when evaluating the appropriateness of mitigating actions applied. The AT also considered the extent to which steps taken to promote tax transparency in recent years have reduced the ML risk emanating from tax offences.

20. Given the international nature of financial activities in Liechtenstein, the AT considered the extent of *cooperation* by competent authorities, including the timely and constructive exchange of BO and financial information with foreign counterparts.

21. As the sector presenting the highest residual ML risks, the AT assessed the extent to which risks are assessed and understood by banks, adequate customer profiles are produced and used to monitor activity, and whether suspicion is reported on a timely basis. Given the availability of statutory CDD exemptions, the AT also considered the extent to which they are used and applied,

along with the extent to which CDD is applied independently by banks to TCSP clients. The AT also considered the use of cash in private banking and wealth administration.

22. Since the *establishment and administration of Liechtenstein legal persons and legal arrangements*, as well as of foreign legal persons and arrangements, is one of the most important services offered by the TCSP sector in the country, the AT considered the extent to which personal asset holding vehicles, shell companies, complex structures and bearer shares are used. The AT considered also the types of assets held by legal persons and legal arrangements and depth of control and oversight that is exercised over entities administered in Liechtenstein by TCSPs.

23. In light of these analyses, the AT considered risk classifications, application of CDD measures (including finding out BO), and level of reporting in the TCSP sector and role played by the legal profession in supporting TCSPs.

24. More generally, the AT considered possibilities for the *misuse of legal persons and legal arrangements*, including the extent to which: (i) trusts are established abroad under Liechtenstein law, but which have no other nexus with Liechtenstein; and (ii) legal persons that are not administered by TCSPs may be exposed to misuse by criminals.

25. Whilst the number of *VASPs* registered in Liechtenstein is not large, there is one very large globally active exchange. Accordingly, the AT considered supervision and preventive measures in this new area and extent to which it is possible to confiscate VAs.

26. The country's *supervisory framework* was subject to criticism in the 4th MONEYVAL evaluation round, mostly due to over reliance on inspections conducted by audit firms on behalf of the FMA. As a result, the AT considered the new framework for AML/CFT supervision introduced by the Financial Market Authority in 2018/19, including the adequacy of resources brought in to accommodate these changes.

27. Given the risk that Liechtenstein's financial system could be *misused for TF* purposes, the AT explored the extent to which potential TF risks are understood and prevention measures are in place, the level and quality of TF-related reporting, whether the TF risks are properly understood by law enforcement and whether the absence of TF prosecutions is consistent with the jurisdiction's risk profile. Linked to this, the AT also discussed the extent to which the NPO sector adequately understands its risks and obligations.

28. Given that *a small number of convictions for ML* have been achieved to date in Liechtenstein, the AT evaluated: (i) the extent to which the FIU adequately supports the identification and investigation of complex ML schemes; (ii) the capacity of the competent authorities to progress complex ML investigations and prosecutions; and (iii) whether law enforcement and investigative/judicial results have substantially improved. The team also discussed strategies for prosecution of third-party ML, as well as methods for coordinating and requesting investigative assistance from foreign counterparts.

29. Three areas were identified as allowing for a reduced focus due to the lower risks presented: (i) real estate – considering the lack of access to the property market by foreigners; (ii) online-gambling, licensing for which is subject to a moratorium until 2023; and (iii) dealers in precious metals and stones (DPMS).

1.2. Materiality

30. Liechtenstein has a small open economy and is highly dependent on international trade and finance. It has a diverse national economy which is characterised by a strong industrial and manufacturing sector accounting in 2017 for 37% of employment and 47% of the country's gross valued added (GVA), predominantly metal products, machinery, motor vehicles and trailers, and electrical equipment. General services account for 53% of employment and 33% of GVA followed by financial services at 10% and 20% respectively[3]. It has one of the highest per capita income levels in the world (CHF 180 000 in 2018[4]).

31. Liechtenstein promotes itself as an IFC. In September 2021, it was ranked 72nd in the world (out of 116 centres) by the Global Financial Centres Index. According to the Financial Secrecy Index (2020), the country accounts for 0.02% of the global market for cross-border financial services and is described in that index as a "tiny player". According to estimates by the Boston Consulting Group (2015), Liechtenstein has a share of about 1% of global cross-border assets under administration[5] (compared, e.g., to Switzerland and the United Kingdom/Ireland with around 25% each). Whilst reference is not otherwise made in this MER to these indices, they help to put into perspective the size of the financial sector in Liechtenstein. Whilst the country is a centre for formation of foundations and establishments in particular, the total number of legal persons and legal arrangements is small (less than 25 000 and reducing). Despite its limited size in the context of the global market, Liechtenstein has an internationally oriented financial sector.

32. Client assets under management by banks have risen steadily to over CHF 179 billion in 2020 (CHF 360 billion including foreign group entities) with the banking sector's balance sheet total amounting to CHF 73.3 billion. These compare to gross domestic product of CHF 6.6 billion in 2019[6]. Assets of around CHF 50 billion each are managed by both asset managers and investment funds[7]. The value of bankable assets administered by TCSPs accounts for roughly 20% of assets held by banks based in Liechtenstein. The value of non-bankable assets administered and/or managed by TCSPs is not held.

33. Given the size of the jurisdiction and restrictions placed on business activities, there is no informal sector or shadow economy. Given its geographical position, the jurisdiction has very strong links with Switzerland, Austria, and Germany.

1.3. Structural elements

34. Liechtenstein has all of the key structural elements required for an effective AML/CFT system: political stability; a high-level commitment to address AML/CFT issues; stable

[3] Source: Economic and financial data of Liechtenstein (24 June 2021).

[4] Source: Economic and financial data of Liechtenstein (24 June 2021).

[5] Source: Economic and financial data of Liechtenstein (24 June 2021).

[6] Source: Economic and financial data of Liechtenstein (24 June 2021).

[7] Source: Economic and financial data of Liechtenstein (24 June 2021).

institutions with accountability, integrity, and transparency; governmental rule of law; and a capable, independent, and efficient judicial system.

35. In 2020, the Council of Europe's Group of States against Corruption (GRECO) assessed the effectiveness of Liechtenstein's corruption prevention in respect of members of parliament, judges, and prosecutors (fourth evaluation round). GRECO reported that: (i) there are virtually no known instances of corruption-related practices involving persons holding these public offices; (ii) the legislative process is globally transparent, and regularly includes public consultation on proposed legislation; and (iii) significant efforts had been taken to adapt legislation to international requirements concerning incrimination of various aspects of corruption. All recommendations set out in GRECO's (third) evaluation report had been fully implemented.

36. Over the past 20 years, Liechtenstein has shown its commitment to fighting ML/FT. It has been an active member of MONEYVAL since 1999 and, as part of its integrated Financial Centre Strategy, has adopted a clear strategy for transparency and tax cooperation with the Liechtenstein Declaration (2009). In the updated Financial Centre Strategy published in February 2019, the Government further fleshed out its strategic objectives and implementation of strategic measures. The effective fight against ML, predicate offences for ML, organised crime and FT is part of the strategy.

1.4. Background and Other Contextual Factors

37. Liechtenstein has a mature and sophisticated AML/CFT system dominated by 12 banks that has recently been extended to cover VASPs. The BO of the customer base for banks and other sectors is predominantly resident (in order) in Liechtenstein, Switzerland, Austria, and Germany. As the private sector aligns its offering with the financial market strategy, domestic growth has been limited and some banks have looked to generate new business by establishing foreign subsidiaries, branches, and representative offices, e.g., in Dubai, Hong Kong and Singapore. Consolidated client assets under administration by banks in 2020 totalled CHF 365.4 billion against CHF 179.2 billion excluding foreign group companies.

38. The country has also looked for new business from financial and regulatory technology markets as technology companies with digital products are increasingly seen on the financial market. As a result, work on blockchain legislation culminated in the Token and TT Service Providers Act (TVTG) which entered into force on 1 January 2020, making Liechtenstein the first country in the world to have comprehensive regulation and a supervisory system in the area of the token economy.

39. Linked to this, a Regulatory Laboratory/Financial Innovation Group, a board directly overseen by the managing board of the Financial Market Authority, was created in June 2018. Despite many potential applicants for VASP registration, only a relatively small number have subsequently submitted applications.

40. Liechtenstein has been used to evade tax, particularly on account of banking and other professional secrecy and the fact that it provided only very limited administrative assistance in the field of taxation until 2009. Since 2009, Liechtenstein has been actively involved in combating international tax evasion and strengthening co-operation in tax matters in general. Liechtenstein abolished tax secrecy for foreign customers in 2009 and, since then, has implemented

international tax transparency standards developed by the Organisation for Economic Cooperation and Development (OECD) and the Global Forum, including automatic exchange of financial account information. By joining the Convention on Mutual Administrative Assistance in Tax Matters, Liechtenstein has become part of a worldwide network for the exchange of tax information (on request, automatically and spontaneously) with more than 140 signatory countries. Furthermore, the country does not have any harmful tax regimes according to the OECD Forum on Harmful Tax Practices and EU Code of Conduct Group (Business Taxation), and peer reviews by the Global Forum have confirmed a high level of compliance, including with the Common Reporting Standard on automatic exchange of information.

41. At the level of domestic legislation, "serious tax offences" have been predicates to ML since 2016. Serious tax offences, in terms of Liechtenstein criminal law, are: (i) tax fraud; (ii) VAT fraud; and (iii) qualified tax evasion related to VAT (when for VAT evasion purposes one or more persons are recruited or when such evasion is committed on a professional basis). Tax fraud differs from tax evasion since it is considered committed only when there is (ab)use of false, falsified, untrue account books and other documents, with intent. Simple tax evasion, in which income is not declared or not fully declared in a tax return, does not constitute a predicate offence to ML in Liechtenstein. In this respect, the amount of tax evaded is not relevant for the qualification of the tax offence.

42. There are also strict controls on who may live and trade in Liechtenstein and buy real estate in the country.

1.4.1. AML/CFT strategy

43. A national AML/CFT strategy was adopted by the Government in July 2020. The Strategy to combat ML, predicate offences to ML, organised crime, and the FT (AML/CFT Strategy) follows the principles of the Financial Centre Strategy and is part of that strategy. Four strategic objectives have been defined: (i) effective implementation of international obligations and standards to combat ML and TF, taking into account the specific risks identified for Liechtenstein; (ii) risk-based focus to increase effectiveness in combating ML and TF and improve the risk management by persons subject to the DDA; (iii) effective prosecution of ML and TF; and (iv) further intensification of national and international cooperation and coordination and domestic exchange of information. The strategy forms the basis for the Action Plan, which is updated on a continual basis.

44. In order to support objective (iii) above, a Confiscation and Asset Recovery Policy was adopted by the Government in November 2020. Under this policy, Liechtenstein commits to depriving criminals of any material benefit from their crimes by aggressively pursuing the freezing and seizure and the forfeiture and confiscation of property, whether held by perpetrators or by third parties. This calls for close cooperation between all competent authorities and for law enforcement authorities to make maximum use of all legal possibilities.

1.4.2. Legal & institutional framework

45. The **PROTEGE WG** (established in 2013) is as a permanent national inter-office working group on combating ML, TF and proliferation financing and is responsible for coordination and cooperation in these areas. The group also has a strategic role - preparing the AML/CFT Strategy

and Confiscation and Asset Recovery Policy for the Government - and coordinates legislative proposals. The following are permanent members of the PROTEGE WG: Ministry of General Government Affairs and Finance (Chair); the Financial Market Authority; the FIU; the OPP; the Court of Justice; the National Police; the Fiscal Authority; the Office of Justice; and the Office for Foreign Affairs.

46. The institutional framework involves a broad range of authorities.

Ministries:

47. The **Ministry of General Government Affairs and Finance** is responsible for the Financial Centre Strategy, including countering the abuse of the financial centre for criminal purposes. The Ministry chairs the PROTEGE WG.

48. The **Ministry of Infrastructure and Justice** is responsible for civil law, including the Persons and Companies Act (PGR), criminal law, mutual legal assistance, extradition and transit, and enforcement of sentences.

49. The **Ministry of Home Affairs, Economy and Environment** exercises authority over the National Police. It also has legal responsibility for cross-border cash transportation control.

50. The **Ministry of Foreign Affairs, Education and Sport** is involved in the ratification of relevant treaties and in the implementation of international sanctions.

51. **Government Legal Services** is responsible for the implementation of international sanctions into national law.

52. The **Office for Foreign Affairs** is involved in the ratification of relevant treaties in the area of AML/CFT and is responsible for coordinating the implementation of international sanctions.

53. The **Office of Justice** - **Judicial Affairs Division** is Liechtenstein's central authority for requests for international mutual legal assistance in criminal matters. It transmits requests to the Court of Justice and submits responses to requests. The **Commercial Register Division** of the Office of Justice is responsible for maintaining the commercial register in which public limited companies, foundations, establishments, and other legal entities are entered. The Office of Justice also houses the **Foundation Supervision and AML Division**, which includes the **Foundation Supervisory Authority (STIFA),** and maintains the central register of BO information. STIFA supervises common-benefit foundations (also referred to as public-benefit or non-profit foundations). Private-benefit foundations may elect to place themselves under STIFA supervision. According to its legal mandate, STIFA ensures that foundation assets are managed and distributed in accordance with the foundation's purposes.

54. The **Office of Economic Affairs** is responsible for issuing casino licences.

Criminal justice and operational agencies:

55. The **Financial Intelligence Unit (FIU)** is an independent unit established for receiving, analysing, and disseminating SARs/STRs. It also produces financial intelligence products and conducts operational and strategic analysis. It is the central office for receiving and analysing information to identify indications of ML, predicate offences of ML, organised crime, and TF. It has two departments, operational and strategic analysis, and designated staff for international affairs. It is also the competent authority for implementing and enforcing targeted financial

sanctions (TFS) and supervises the enforcement of coercive measures in line with the Ordinance on Measures against Certain Persons and Organisations to fight Terrorism.

56. The **National Police** are responsible for investigating all offences in Liechtenstein, including ML, predicate offences, TF, and TFS violations. One unit (the Financial Crime Unit) deals specifically with financial and economic affairs and is part of the Crime Investigation Division (which deals with ML/TF matters).

57. The **Office of the Public Prosecutor (OPP)** prosecutes, indicts, and argues the indictment before the competent court ex officio with respect to all reported offences. It safeguards the interests of the state in the administration of justice, in particular with respect to the administration of criminal justice and mutual legal assistance in criminal matters. In the exercise of its responsibilities, it is independent of the courts and represents the state before the courts.

58. Four judges of the **Court of Justice** serve as investigating magistrates, having authority to issue legal orders, such as production orders and search and arrest warrants. They are responsible also for freezing and seizure actions used to prevent the dissipation of assets.

59. The **Fiscal Authority** is responsible for the implementation of tax information exchange with foreign tax authorities (exchange on request, automatic and spontaneous) on the basis of international agreements.

60. In line with Liechtenstein's membership of the Swiss customs territory, the **Swiss Border Guards Corps** is responsible for applying border controls at the Austrian-Liechtenstein border. The National Police have delegated border cash control powers to the Border Guards.

Financial and non-financial supervisors:

61. The **Financial Market Authority (FMA)** is an autonomous establishment under public law with its own legal personality. Its objectives includes implementation of, and compliance with, recognised international standards, safeguarding financial market stability, protecting customers, and preventing abuse. The FMA is an integrated supervisor, responsible for the prudential supervision of the financial sector and AML/CFT compliance by all FIs, DNFBPs, and VASPs, except lawyers.

62. The **Chamber of Lawyers** is a corporation under public law and licences lawyers. It is also responsible for safeguarding the honour, reputation, and rights of the legal profession, and supervising compliance with duties. Since 2017, the Chamber of Lawyers has been responsible for monitoring compliance by lawyers with AML/CFT requirements.

63. The Due Diligence Act (DDA) and subordinate ordinance – the Due Diligence Ordinance (DDO) - are the main statutes dealing with AML/CFT matters. Inter alia, the DDA covers preventive measures and reporting, AML/CFT supervision and regulates the international exchange of information. The DDA and DDO are supplemented by guidelines (including instructions) which are considered to be enforceable means (see R.34 in the TC Annex). The FIU Act provides for the establishment and functioning of the FIU.

64. Other relevant laws include sectorial laws regulating the financial and DNFBP sectors, the CC, the Code of Criminal Procedure (CPC) - which deals with tracing and freezing of assets, the

International Sanctions Act (ISA), the Persons and Companies Act, the Act on the Register of the BOs of Legal Entities (WwbPG), and the Mutual Legal Assistance Act (MLA Act).

65. The cooperation and coordination mechanism used to assist the development of policies is explained under Chapter 2.

1.4.3. Financial sector, DNFBPs and VASPs

Financial sector and DNFBPs.

66. The following table shows the number of financial market participants from 2014 to 2021:

Table 1.1: numbers of registered FIs, DNFBPs and VASPs

Type	Number of entities at year end	2016	2017	2018	2019	2020	2021 (Sept.)
FIs	Banks	15	15	14	14	14	12
	Investment firms	1	1	1	0	0	0
	Payment institutions	1	2	1	1	1	1
	E-money institutions	2	2	3	5	4	3
	Fund management companies (individual portfolio management)	2	5	7	7	6	6
	Funds*	0	0	684	613	643	676
	Asset managers	116	109	109	104	102	101
	Life insurance undertakings	21	21	21	21	19	18
	Life insurance intermediaries	51	43	30	31	30	21
DNFBPs	Lawyers	28	51	24	27	21	
	TCSPs**	189	188	184	188	185	188
	Tax consultancy***	0	0	0	1	1	1
	Accountants***	0	0	6	8	7	7
	Estate agents	0	7	3	4	6	6
	Dealers in high value goods	7	3	3	4	6	7
	Casinos	0	2	2	4	5	5
VASPs	Crypto exchange/ VASPs****	0	1	3	3	13	10

* Until 2017, fund management companies (rather than individual investment funds) were subject to the DDA.

** The figures refer to active TCSPs, under whose umbrella individual licence holders (trustees, trust companies and Art.180a persons) operate. The FMA conducts consolidated AML/CFT inspections in which the individual licensees are jointly inspected on the basis of their legal/economic links. The number of individual licence holders was as follows: 2016: 619; 2017: 617; 2018: 638; 2019: 665; 2020: 668; and 2021: 649.

*** Tax consultancy and accountants have been subject to the DDA since 1.9.2017.

**** From 2017 until end of 2019 only crypto exchanges were subject to the DDA. As of 2019, all VASPs are subject to the DDA.

67. It is not possible to give exact numbers of licenced tax consultants, accountants, estate agents and HVGDs due to the use of non-standardised wording for recording commercial ventures/occupations provided by applicants to the Office of Economic Affairs. For example, an accountant that is also a tax consultant will be reported only once (as an accountant or as a tax consultant).

68. As mentioned above, the financial sector is dominated by 12 banks, the focus of which remains mainly on international wealth administration. In recent years, domestic **banks** in

particular have benefited from the strong growth of foreign subsidiaries and branches. Liechtenstein banks have not only increased their foreign presence, but they have also occasionally attracted foreign investors. Banks are also increasingly trying to position themselves through special and innovative services, e.g., the development of relevant expertise in the field of regulated blockchain banking services.

69. The core business of asset managers in the **securities sector** is portfolio administration and provision of investment advice. Target customers are mainly private customers, and the majority of institutional clients are Liechtenstein investment funds, for which asset management (portfolio management) is provided.

70. The investment fund sector focuses on the creation and administration of investment funds governed by EU legislation (UCITS Directive and AIFM Directive).

71. **Insurance companies** are increasingly diversifying away from unit-linked life insurance. Non-life insurance products now account for more than 50% of premium volume written, given the low interest rate environment. Liechtenstein offers insurance undertakings direct market access to the countries of the EEA and to Switzerland.

72. The **TCSP sector** has seen occasional mergers of medium-sized to small trust companies. In order to preserve traditional smaller TCSPs – which are subject to increased compliance costs - a shared service centre has been established to undertake administrative and technical tasks of client management allowing trustees to focus on core business.

73. Given the peculiarities of the TCSP sector in Liechtenstein, lawyers give advice on the establishment of legal persons, legal arrangements, or structures only under the umbrella of a TCSP engaged in establishing legal persons or trusts. Trustees are also licensed to provide tax advice, and therefore there is little activity in this respect outside TCSPs. Accordingly, the number of lawyers and accountants registered to provide services for AML/CFT purposes is much lower than might be expected in an IFC and number of transactions by lawyers within the scope of AML/CFT requirements averages around just ten per year.

74. In 2017, the first two licences for land-based **casinos** were approved. The market has steadily grown since then and there are five currently licensed. Growth is supported by a large regional catchment area (good transport links) with high purchasing power and business-friendly framework in Liechtenstein (e.g., smoking rules and dress code). There have been no online developments as a result of a licensing moratorium – extended until the end of 2023.

75. The **VASP sector** is still nascent with a limited number of entities. On 1 January 2021, there were eight registered VASPs and three token issuers (latter category subject to notification requirement) which are subject to the ongoing AML/CFT supervision of the FMA. The structure of the VASP sector is very inhomogeneous. On the one side there are small token issuers, which issue less than CHF 5 million per year in their own name and on the other side there is one large exchange which has a significant number of customers running into hundreds of thousands.

76. Based on materiality and risk of services and products offered by the banks and assets held by them, the banking sector is weighted as most important.

77. Among non-bank FIs, fund management and asset managers are weighted as highly important taking into the account the volume of assets under management, business relationships with HNWIs and application of exemptions under the DDO, when they are heavily

reliant on subscribing intermediaries (banks). Insurance undertakings are also weighted as highly important given the fact that business relationships involve persons residing abroad (including residents of third countries), often HNWIs. All other FIs are weighted as moderately important.

78. Amongst DNFPBs, the TCSP sector is the largest sector, as the establishment and administration of Liechtenstein legal persons and legal arrangements, as well as of foreign legal persons, is one of the core services offered in Liechtenstein. TCSPs play an important gatekeeper role since many of their clients hold accounts in the banking sector and account for a high level of customer deposits. Banks use TCSPs as a facilitator to collect much of the CDD that they are required to undertake when a client of a TCSP establishes a business relationship. Additionally, most Liechtenstein legal persons are required to appoint a qualified member to sit on the board of the governing body, which makes TCSPs a critical gatekeeper for legal persons. As the TCSP sector plays such a dominant role in Liechtenstein in terms of assets, number, and types of clients and because of the risk of services offered (e.g., creation and management of complex corporate structures and trusts), it is weighted as most important.

79. All other DNFBPs (except real estate brokers and DPMS) are weighted as moderately important, while real estate brokers and DPMS, given the small size of these sectors and state's strict controls over real estate transactions, are weighted as less important.

80. Liechtenstein has introduced comprehensive regulation of the VASP sector which is dominated by one large VASP. Given the following, this sector is weighted as highly important: (i) inherent risk of VAs, e.g., anonymity; (ii) legal requirements are new; (iii) there are difficulties in the process of implementation of the travel rule in practice; (iv) there are a substantial number of legacy customers from different countries at one large entity[8] where accounts have been established without full CDD; and (v) the high number of SARs/STRs submitted.

1.4.4. Preventive measures

81. As mentioned above, the DDA and DDO are the main statutory instruments through which preventive measures are applied in line with the FATF Recommendations (see TC Annex). They are supplemented by guidelines (including instructions) – see R.34.

82. The following activities which are covered by the FATF definition of FI are also not subject to the DDA: (i) lending (own funds only); (ii) financial leasing; and (iii) issuing and managing paper-based means of payment. The following activities which are covered by the FATF definition of DNFBPs (as applied by R.22 and R.23) are not subject to the DDA: (i) lawyers, law firms and accountants preparing for or carrying out transactions for clients with respect to the creation, operation or management of legal persons or arrangements; and (ii) notaries. There is no general regulation or supervision of transfers of VAs which is called for by the FATF Recommendations.

83. Whereas fund managers are licensed and supervised for prudential purposes, they are not subject to the DDA or supervision for AML/CFT purposes (except in the case of individual portfolio management provided by fund management companies). Instead, underlying

[8] VASP with around 750,000 customers and 4 billion transactions volume in 2020 that accounts for almost 90% of the sector.

investment funds are licenced and subject to supervision for AML/CFT purposes. In the case of externally managed funds, responsibility for undertaking due diligence at investment fund level is delegated by law to the management company. There is a very small number of foreign investment funds (four out of more than 600) which are solely administered in Liechtenstein, that have not been supervised for compliance with the DDA by the FMA.

84. Liechtenstein AML/CFT requirements are not applied to business conducted remotely in Liechtenstein by EEA FIs or Swiss insurance undertakings and intermediaries. Home country AML/CFT requirements (EEA or Swiss) apply in these cases.

85. In addition to DNFBPs covered by the FATF Recommendations, the following are subject to the DDA: (i) providers of online gambling; (ii) members of tax consultancy professions insofar as they assist clients in the planning and execution of specified financial and real estate transactions; (iii) letting activities of estate agents where monthly rent amounts to CHF 10 000 or more; (iv) persons trading in goods (over and above DPMS) that receive payment in cash or by VA or a token and the amount involved is CHF 10 000 more; (v) persons trading in works of art or acting as intermediaries in the trade of works of art, including art galleries or auction houses, provided that the value of a transaction amounts to CHF 10 000 or more; and (vi) persons who, on a professional basis, hold foreign assets in safe custody and rent out premises and containers for the storage of valuables. These additional areas of regulation are based on EU Anti-Money Laundering Directives (AMLDs) and are not linked to particular risks identified in Liechtenstein.

1.4.5. Legal persons and arrangements

86. The formation and administration of legal persons and legal arrangements has a decades long tradition in Liechtenstein. In the first half of the last century, the Persons and Companies Act came into force, which also introduced the Anglo-American legal institution of the trust. Combined with business-friendly tax rules, the sector became important in the second half of the last century. In recent years, the number of legal persons and legal arrangements registered or otherwise domiciled in Liechtenstein has fallen dramatically.

87. In addition to legal forms recognised in the Persons and Companies Act, national law also allows for the incorporation of the following European legal entities: (i) European Company (legal person); (ii) European Cooperative Society (legal person); and (iii) European Economic Interest Grouping.

88. The only legal arrangement that can be created under Liechtenstein law is the trust; all other entities are classified as legal persons.

89. The below table outlines the number of legal persons and arrangements in Liechtenstein as at the end of 2020:

Table 1.2: Registered legal persons and arrangements.

Legal form	31.12.2020
Non-registered foundation (deposited foundation)	8 693
Establishment	4 983
Public limited company	4 917
Registered foundation	1 759
Registered trust	1 692

Limited liability company	778
Trust enterprise	631
Association	343
Non-registered trust (deposited trust)	86
Limited partnership	27
Cooperative society	25
General partnership	21
European Company	13
European Cooperative Society	4
Partnership limited by shares	2
European Economic Interest Grouping	1
Total	23 975*

* Not included are 542 sole proprietorships, 11 public foundations and 11 public establishments.

90. The foundation, the establishment (Anstalten), and the public limited company are the most common legal forms in Liechtenstein. Non-registered foundations are the most numerous. The total number of legal entities has decreased by more than 68% in the past 13 years. This substantial decrease is due to: (i) the Liechtenstein Declaration of 2009, with which Liechtenstein committed itself to implementing the OECD global standards on transparency and exchange of information for tax purposes; (ii) the Government Declaration of 2013, in which Liechtenstein confirmed its commitment to the applicable OECD standards for tax cooperation; and (iii) considerable increases in management and administration costs due to additional regulatory requirements. In addition, implementation of the FATF Recommendations and EU AMLDs has also contributed to the decline.

91. The business model of formation and administration of legal entities is the core business of TCSPs. Whilst Liechtenstein legal entities are used by persons residing in Liechtenstein, they are mainly used by non-residents.

92. In addition to formation and administration of Liechtenstein legal entities, TCSPs also offer to their clients the formation and administration of foreign legal entities. In a very large number of such cases, a Liechtenstein legal entity, usually a foundation, serves as the holding body.

1.4.6. Supervisory arrangements

93. As explained earlier, the FMA is an integrated supervisor, responsible for the prudential supervision of the banking, securities, and insurance and pension fund sectors in line with international standards. The FMA is also responsible for AML/CFT supervision and ensuring compliance with the regulatory framework by FIs, VASPs, Casinos and DNFBPs, except for lawyers. It is independent from the Government and operates as an autonomous institution.

94. Since 2019, responsibility for AML/CFT supervision within the FMA has rested within newly created AML/CFT and DNFBP Division, comprising of two separate sections: (i) the AML/CFT Section (responsible for supervision of all persons subject to DDA); and (ii) the DNFBP Section (responsible for prudential supervision of DNFBPs and AML/CFT enforcement of all persons subject to the DDA). Staffing number are covered under IO.3.

95. Since 2017, the Chamber of Lawyers has supervised lawyers for compliance with AML/CFT requirements. It is a self-regulatory body, with some limited oversight by Government.

96. The FMA is the competent authority for granting, amending, and withdrawing licences for FIs, TCSPs and VASPs. Lawyers are licensed by the Chamber of Lawyers. Other types of DNFBPs, except TCSPs, are licensed by the Office of Economic Affairs.

97. The Commercial Register Division is, inter alia, responsible for Liechtenstein's public register of legal persons and legal arrangements. In 2020, it had 13.85 FTE staff. The Foundation Supervision and AML Division of the Office of Justice supervises the management of, and distributions by, common-benefit foundations (since 1 April 2009) and maintains Liechtenstein's central register of BO (since 1 August 2019). In 2020, it had 5.3 FTE staff. Since October 2021, the Foundation Supervision and AML Division has also had responsibility for maintenance of Liechtenstein's central register of bank accounts.

1.4.7. International cooperation

98. Given its context as an IFC and predominantly foreign nature of predicate offences to ML (most prevalently fraud, criminal breach of trust and embezzlement, tax offences, corruption, and drug related offences) international cooperation plays an important role for Liechtenstein in the overall framework of its AML/CFT efforts. Since 2016, Liechtenstein has provided MLA for a certain set of fiscal offences (tax fraud and qualified tax evasion) if the dual criminality test is met, i.e., if the circumstances of the case described in the MLA request would be punishable by a court according to Liechtenstein legislation. In the event that the dual criminality requirement is not met, administrative assistance would still be granted. The administrative assistance procedure between competent authorities neither differentiates between tax offences and criminal tax offences nor between simple or qualified tax offences. Criminal tax cases are eligible for official assistance if the foreign judicial authority is designated as the competent authority.

99. The main international partners of Liechtenstein are Austria, Germany, and Switzerland, while cooperation with other countries is also in place, though to a lesser extent. In general, Liechtenstein has a comprehensive legal framework to provide international cooperation to its counterparts either through MLA or other forms of international assistance. International cooperation is governed by the MLA Act and various international conventions ratified by Liechtenstein. The Office of Justice is the Central Authority in Liechtenstein for both MLA and extradition requests, though requests may be addressed directly to the Court of Justice. Only those requests that are not governed by the ECMA/Schengen Agreement or special bilateral treaties (e.g., Austria, Germany, Switzerland, or the U.S.) go through diplomatic channels.

100. Liechtenstein has entered into an Agreement on Operational and Strategic Co-operation with the European Police Office (Europol) and participates in the Secure Information Exchange Network Application (SIENA) as well as the Camden Asset Recovery Inter-Agency Network (CARIN). Liechtenstein has also been a member of INTERPOL since October 1960. Liechtenstein has furthermore concluded a trilateral treaty on police cooperation with Switzerland and Austria.

2. NATIONAL AML/CFT POLICIES AND COORDINATION

2.1. Key Findings and Recommended Actions

Key Findings

Immediate Outcome 1

a) Risks have been assessed in a frank and impartial way and, overall, the authorities have demonstrated a good broad and convergent understanding of core ML/TF risks. Whilst there is a scope for a more comprehensive understanding of risk in some particular areas (described below), this only requires refinements to a well-established risk process.

b) Banking and TCSP activities are identified as presenting the highest ML risks. Residual risk ratings for these and other sectors and related analyses demonstrate a good broad understanding of ML risk, including risks presented by managing the wealth of high-net-worth individuals. The authorities have also conducted a comprehensive assessment of ML risk inherent in legal persons and legal arrangements. This assessment also demonstrates a good broad understanding of risk, though it appears to overstate the importance of one particular mitigating measure. The country has demonstrated understanding to some extent of the risk that is presented by the operations of foreign branches and subsidiaries of Liechtenstein-based banking and TCSP groups, e.g., in the case of banks, group risks are understood by the FMA.

c) Even though the risk of misuse of Liechtenstein's financial sector to launder the proceeds of tax offences committed abroad has been recognised, the extent of the threat has not been estimated. Two other ML threats have not been fully examined these being: (i) the extent to which prominent global offences that have a transnational element may be laundered through the financial system in Liechtenstein and (ii) understanding of transactional links to countries presenting a higher ML risk.

d) Some important inherent ML risks have not been considered which affect understanding of risk: (i) whilst the FMA now holds valuable information about TCSPs, this does not include data on the types and location of non-bankable assets that are administered by TCSPs - often held through complex structures; (ii) information is not held on the profile of customers of banks that subscribe for units in non-private investment funds; and (iii) there has been limited analysis of the use of cash.

e) Recent changes to Art. 165 of the CC - to include tax savings as asset components subject to ML - have largely curtailed use in the private sector of shell companies, which is conscious of the higher risk of such companies being used to make transactions now criminalised under the CC. However, understanding of how residual risk has changed in this area is rather limited.

f) Extensive use is made of data collected by the FMA to understand TF risk. Whilst the analysis and consequent understanding of transactional links to countries presenting a higher TF risk is insufficient, this is considered to have only a minor effect on risk understanding.

g) ML/TF risks, as acknowledged and analysed in national risk assessments, are addressed successfully by national AML/CFT policies and activities. The country's action plan does not include any explicit action to examine and estimate the extent of use of Liechtenstein's financial sector to launder the proceeds of tax offences committed abroad. The authorities would also benefit from a set of formally documented high-level national policies pitched between strategic objectives and detailed actions - to guide competent authorities in the delivery of their statutory functions.

h) Cases triggering the application of EDD and simplified measures are consistent with risks identified in NRA II. Some exemptions from the application of preventive measures are in place that are not supported by a risk assessment at country level.

i) Objectives and activities of the competent authorities are commensurate with risks identified in NRA II and policies. In particular, the supervisory system in Liechtenstein was completely redesigned in 2018/19 and FMA's risk-based approach strengthened. Efforts made were linked to findings in the NRA and appear to have had some success since understanding of risk and the application of AML/CFT preventive measures are now generally good in the banking and TCSP sectors (see chapter 5).

j) Cooperation and coordination among stakeholders is effective and constitute one of the strengths of Liechtenstein. The country applies a "whole of government approach" – whereby there is close and effective cooperation in the development and implementation of policies and activities between competent authorities through working groups.

k) Based on efforts taken to share results, the private sector demonstrated a high level of awareness on NRA findings.

Recommended Actions

Immediate Outcome 1

a) Liechtenstein should conduct additional studies to examine and estimate the extent of ML threats associated with tax offences committed abroad. In line with the country's action plan, it should continue to improve its understanding of ML/TF threats presented by transactional links to countries presenting a higher ML risk. Follow-up action should be taken as necessary.

b) Liechtenstein should consider collecting the following additional information in order to support its analyses of inherent risk: (i) types and location of non-bankable assets that are administered by TCSPs (e.g., foreign operational subsidiaries, high value goods and real estate); (ii) profiles of underlying investors in investment funds that benefit from CDD exemptions; and (iii) use of cash and prepaid cards, e.g. economic sectors presenting greater exposure and reasons, recurrent use of cash above certain thresholds, use of ATMs in countries that neighbour conflict zones, and trends. Follow-up action should be taken as necessary.

c) Liechtenstein should examine ML threats deriving from a wider range of prominent global offences (in addition to those identified on the basis of SARs/STRs, MLA etc), that have a

transnational element and so may be laundered through the financial system in Liechtenstein, e.g., by using typologies on ML pathways in IFCs, findings and recommendations available from public reports on risks emanating from predicate offences prominent globally, and more proactive input from the private sector.

d) Liechtenstein should analyse the risk that is presented by the operations of foreign branches and subsidiaries of domestically headquartered banking and TCSP groups, making use of information already held by the FMA for banking groups. Follow up action should be taken as necessary.

e) Liechtenstein should formally document its high-level national policies - to guide competent authorities in the delivery of their statutory functions, e.g., prioritisation of typologies linked to the overall risk profile of the country when handling financial intelligence.

f) Liechtenstein should review exemptions from CDD obligations (including those supported by European guidelines) to ensure that they are supported by country assessments of risk and amend as appropriate.

101. The relevant Immediate Outcome (IO) 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, and elements of R.15.

2.2. Immediate Outcome 1 (Risk, Policy and Coordination)

2.2.1. Country's understanding of its ML/TF risks

102. The authorities have demonstrated a good broad and convergent understanding of core ML/TF risks in the financial, TCSP, casino and VASP sectors and sufficiently broad understanding of risks in other sectors too. This is assisted by the fact that the core elements of products and services provided to manage wealth – private banking and asset management - have not changed significantly over the years, even if the regulatory environment linked to them has. Whilst there is scope for a more comprehensive understanding of risk in some particular areas (see limitations in scope and gaps noted below), this requires refinements to a well-established risk assessment process that is already based on a comprehensive methodology, multi-agency engagement and proactive data collection, rather than a thorough change of approach. Risk assessments are considered by the AT to be up-to-date, frank, and impartial.

Methodology for assessing ML/TF risk

103. Liechtenstein first published a national risk assessment (NRA I) in 2016 - based on data collected for 2013 to 2015. An executive summary document setting out the results and accompanying explanations was published in July 2018. Since then, a second NRA has been undertaken in three component parts: (i) ML (July 2020); (ii) TF (May 2020); and (iii) VAs (January 2020 – updated August 2021) (collectively referred to as NRA II). This risk assessment relies on a more extensive data collection for 2016 to 2018 – including data not available for the first assessment, e.g., cross border flows and residence of BOs of customers (see below). NRA II

supersedes NRA I, except for sectoral assessments of some non-financial sectors (including lawyers, accountants (including auditors and auditing companies), dealers in goods, and real estate agents) that were not repeated in the second iteration of the risk assessment on the basis that no changes had been observed in these sectors and earlier assessments of lower risk. The AT considers this method to be justified and in line with a risk-based approach. An executive summary of parts (i) and (ii) of NRA II was published in January 2021. A further NRA update is to be conducted in the course of 2022.

104. Separate risk assessments have also been conducted for: (i) NPOs (May 2020) – in order to identify those considered to be most at risk of TF abuse in accordance with R.8; and (ii) legal persons and legal arrangements (May 2020) – to analyse ML threats, inherent risks, and risk-mitigating measures in accordance with R.24.

105. The World Bank Methodology was used to prepare NRA I, whereas NRA II draws more on FATF guidance, to allow the authorities to better focus on the peculiarities of an IFC. NRA II examines threats/inherent risks and vulnerabilities and assigns a final ML risk rating (residual risk) to each examined sector and overall TF risk rating (residual risk), based on the interplay between these factors. Both methodologies are comprehensive and support the country's understanding of risk.

106. All of the necessary public stakeholders have been involved in the NRA process through an effective coordination mechanism (see R.1), and the authorities have explained that there was proactive engagement of the private sector in the preparation of NRA I. Notwithstanding the proactive level of engagement by the FMA at that time, the authorities have not provided sufficient information on the extent of private sector engagement in this first iteration of the risk assessment, e.g., numbers involved in NRA working groups, the roles they played, and input they provided and so it is not possible to determine the extent of engagement or to which the sector was able to contribute to the country's understanding of risk. In the course of NRA II, there was more limited engagement with the private sector. In the initial phase, a questionnaire covering risk was distributed through industry associations and responses provided on a voluntary basis, and the same associations and member firms were later requested to provide feedback on advanced drafts. Whilst such a level of engagement with the private sector may be appropriate for a second iteration of the country's assessment of risk, it has provided fewer opportunities for emerging ML trends to be identified.

107. In 2020, the FIU established a Public Private Partnership (PPP) forum with the Banking Association. This additional mechanism adds further to the authorities' understanding of risk on an ongoing basis, allowing them to develop a better inside view of the banking sector. Regular topic-based meetings are held and have helped, e.g., to identify signs of growing interest in serving VASPs.

108. As mentioned above, significant efforts were employed to collect a broader set of data for analysis under NRA II. In particular, extensive use was made of the FMA's Risk Analysis System, which requires prescribed information to be provided to the supervisor on an annual basis. In addition to general factors, e.g., data on customer, product, and service risk, valuable sector specific data is also collected, e.g., total volumes of cash and non-cash deposits and withdrawals. This means that the FMA and other authorities have a good basis for understanding inherent sectoral risks. In particular, comprehensive data is collected on the residence of BOs (all sectors) and origin of incoming and outgoing fund flows by country.

Country's understanding of ML risk

109. Liechtenstein describes and promotes itself as an internationally focused financial centre/IFC. As such, the country understands that it is primarily exposed to external ML threats as non-residents seek to transfer criminal proceeds to, or through, Liechtenstein, particularly through its banking system or through the use of TCSPs. The main ML threats identified by Liechtenstein arise from laundering of proceeds of fraud and corruption (high threat), tax-related crimes (medium-high threat), narcotics crimes (medium threat), and theft, insider dealing, and market manipulation (medium-low threat). Since the level of domestic criminality is low, the threat that domestic proceeds may be laundered is considered to be negligible.

110. The authorities recognise and understand the inherent risk of services offered in the private sector. In particular, these services are offered to non-resident high-net-worth individuals, some of whom are "influential"[9], and they make use of complex structures (including mixed groups of legal persons and arrangements) established by TCSPs.

111. Based on the methodology and factors outlined above, residual ML risks have been assessed in NRA II as follows: (i) medium-high for banks and TCSPs; (ii) medium for insurance undertakings, insurance intermediaries, asset managers and investment funds; and (iii) medium-low for casinos (online gambling is not permitted[10]). With regard to the VASP sector, ML risk is assessed as medium-high for VASP exchanges, medium-low for issuers, and medium for other regulated VASPs. These residual risk ratings and linked NRA analysis demonstrate a good broad understanding of core ML/TF risks for the financial, TCSP, casino and VASP sectors, including risks presented by managing the wealth of high-net-worth individuals.

112. In NRA I, lawyers and DPMS were rated medium-low, and accountants (including auditors/auditing companies) and real estate agents rated low risk. Whilst the AT has not been provided with risk assessments conducted for these sectors (to explain the basis for the conclusions reached), based on its discussions with the authorities, it is considered that the country has demonstrated a sufficiently broad understanding of ML risks in these sectors. The decision not to reassess these sectors for the purposes of NRA II follows a risk-based approach applied by the authorities in this exercise.

113. As mentioned above, the authorities have also conducted a comprehensive assessment of ML risk inherent in legal persons and legal arrangements that are created in Liechtenstein and those domiciled abroad having a nexus with the country. This is important given that the establishment and/or administration of legal persons and legal arrangements is the core business of the TCSP sector (rated as having a medium/high residual ML risk), though the total number of entities has decreased steadily and significantly in recent years (see Chapter 1). Overall, use of legal persons and legal arrangements (which includes those administered by TCSPs) is considered to present a medium residual ML risk given risk-mitigating measures in place, and, in particular, the requirement to appoint a qualified member (TCSP) to the governing body of those legal persons that are predominantly non-trading and wealth management structures. This residual risk rating and linked analysis demonstrate a good broad understanding of ML risk,

[9] Term taken from European Supervisory Authorities risk factor guidelines.

[10] Moratorium until the end of 2023.

though, as highlighted under Chapter 7 (IO.5), there are concerns over the continued limited level of supervision of TCSPs and so impact of this mitigating measure may be overstated in the final assessment of residual risk.

114. The AT has noted a high level of agreement amongst the authorities and private sector on conclusions reached for NRA II (both ML and TF). Acknowledgment of inherent risks in the private sector has increased significantly since NRA I, where opinions were less uniform.

115. During the period under review, the authorities discussed whether to prohibit or regulate VA activities in Liechtenstein. A decision was taken to regulate the sector (including issuers where an increased level of risk had been identified), a risk assessment was conducted (which involved internationally leading experts in the VA field), a regulatory and supervisory framework introduced (see R.15) and number of steps taken to address inherent risks, e.g., training of FIU analysts, use of VA software to monitor VA sources, and opening of wallets to facilitate the seizure of VAs. The AT has observed that, despite many potential applicants for registration, only a relatively small number have subsequently submitted applications. However, the AT is not satisfied that the authorities considered the risk that is inherent in licensing VASPs not hitherto regulated which have large legacy customer bases.

Limitations in scope of ML risk assessment

116. The scope of NRA II does not extend to: (i) the foreign operations of banking and TCSP groups that are headquartered in Liechtenstein; or (ii) more general ML risks that may affect certain sectors of the wider economy, e.g., use of cash in the industrial and manufacturing sector. Accordingly, the authorities have demonstrated understanding of risk in these areas only to some extent.

117. NRA II is focused on "home" companies and there is limited understanding at country level of the products and services, geographic, and delivery channel risks presented by foreign branches and subsidiaries of banks and TCSPs that are headquartered in Liechtenstein. There are significant and growing operations conducted by banks through foreign branches, subsidiaries, and representative offices, e.g., in Dubai, Hong Kong and Singapore and consolidated client assets under administration by banks in 2020[11] totalled CHF 365.4 billion against CHF 179.2 billion excluding foreign group companies. There are also ten TCSPs that operate outside Liechtenstein through branches and subsidiaries, e.g., in the British Virgin Islands, China, Hong Kong, Panama, Singapore and Switzerland. Numbers employed in banks in Liechtenstein were approximately 2 400, compared to 4 300 abroad[12]. Nevertheless, in the case of banks, such group risks are understood by the FMA.

118. In addition to its financial sector, Liechtenstein also supports a large industrial and manufacturing sector accounting in 2017 for 47% of GVA (see section 1.2). The extent to which this large sector might be vulnerable to ML, if at all, has not been considered, e.g., extent to which cash is used and bribes may be paid to secure contracts or access new markets. Moreover, no information is held on the size of the family office sector, a growth area of business in similar centres, or extent to which such offices may not operate through regulated TCSPs.

[11] Source: Liechtenstein Finance: Thinking in Generations.

[12] Source: Economic and financial data of Liechtenstein (24 June 2021).

Gaps in understanding of ML risk

119. The AT considers that some **threats** have not been fully examined, which affects understanding of risk. These are: (i) the extent to which prominent global offences that have a transnational element could be laundered through the financial system in Liechtenstein; (ii) extent of use of Liechtenstein's financial sector to launder the proceeds of tax offences; and (iii) understanding of transactional links to countries assessed as presenting a higher ML risk. Accordingly, the country is not able to demonstrate that all ML threats are fully understood.

120. There is insufficient understanding of predicate offences, other than those already observed (through SARs/STRs, investigations, MLA requests and press reports) that are prominent globally and which have transnational elements, where proceeds could be laundered through the financial system in Liechtenstein. NRA II also does not generally describe who is presenting a ML threat, where they are, or how they are doing it. Future NRAs would benefit from more intensity of focus in the articulation of threat elements and extent to which Liechtenstein might be targeted, e.g., by using typologies on ML pathways in IFCs, findings and recommendations available from public reports on risks emanating from predicate offences prominent globally, e.g., FATF reports, and more proactive input from the private sector on emerging trends.

121. NRA II considers threats and provides a comprehensive analysis of vulnerabilities posed by tax offences committed abroad, including the absence of tax evasion as an ML predicate offence in Liechtenstein. Some important actions have been undertaken by the authorities since 2009, such as: (i) widening of the criminal provisions relating to serious tax offences which are predicates to ML; (ii) implementation of tax transparency measures and automatic exchange of information with partner jurisdictions; and (iii) availability of administrative assistance in relation to fiscal matters whenever a request for MLA solely refers to tax evasion. These are considered further under Chapters 1 and 8 (international cooperation). On the other hand, there is no estimate of the extent of misuse of Liechtenstein's financial sector to launder the proceeds of: (i) already criminalised tax offences (i.e., qualified tax offences committed after the entry into force of amendments to the CC in January 2016); and (ii) foreign tax evasion. Based on action that has been taken, particularly implementation of tax transparency measures and provision of administrative assistance, the authorities consider that the extent of ML in this respect is limited. Notwithstanding action taken by the authorities to address vulnerability - that has had some positive effect on reducing ML/TF risk in Liechtenstein - the country has not fully assessed the impact that laundering of the proceeds of tax offences may have on its financial system as a whole.

122. The authorities have quantified inflows and outflows of funds on a country-by-country basis and have analysed the rationale and objectives of an extensive number of individual transactions (based on numerous customer file reviews by the FMA). However, the analysis of why funds are received from and sent to countries identified by the authorities as presenting a higher ML risk (CHF 2.7 billion between 2016 and 2018 (0.9% of all transactions)) is rather general and does not consider the reason for, and nature of, such links. Whilst recognising that transactions to and from foreign countries are "largely indirect and rarely transferred directly from the country of origin", the analysis does not consider what the actual exposure may be higher risk countries. Also, there is no analysis of other financial data (apart from a very limited analysis of import-export flows with high-risk countries), e.g., indicators from balance of payments. Accordingly, understanding is rather limited. In order to identify flows that may be

made through intermediary countries, the authorities have explained that use may be made of detailed BO information held for customers (country of residence).

123. The AT considers that some important **inherent risks** have not been considered which affect understanding of risk: (i) whilst the FMA now holds valuable information about TCSPs (e.g. residence of BOs and number which are PEPs), this does not include data on the types and location of non-bankable assets that they administer, e.g. foreign operational subsidiaries, high-value goods and real estate – often held through complex structures; (ii) full information is not held on the extent to which TCSPs hold client funds outside Liechtenstein (see below); (iii) information is not held on the profile of customers of banks that subscribe for units in non-private investment funds using an exemption that is explained under section 2.2.3 below, e.g. whether they are institutional or retail and country of residence; and (iv) there has been limited analysis of the use of cash (see below). Accordingly, the country is not able to demonstrate that all inherent risks are fully understood.

124. Full information is not held on the extent to which TCSPs hold client funds in foreign bank accounts and transactions therefore not subject to ongoing monitoring by a regulated FI in Liechtenstein. This affects understanding of risk. Whilst evidence collected onsite suggests that most bank accounts will be held in Liechtenstein or Switzerland, relationships will be set up in other countries in order to limit credit risk or at the request of a customer. To the extent that TCSPs are banked in Liechtenstein, there will be a regulated FI with knowledge of the country's TCSP sector responsible for monitoring transactions and identifying unusual or suspicious activity, which provides an additional and important layer of oversight and supports the country's understanding of ML/TF risk (e.g., information collected through supervision and through SARs/STRs). Inherent risk increases where customers of TCSPs hold individual signing rights on accounts held outside Liechtenstein (though not common).

125. Whilst risks inherent in the use of cash for private banking/wealth administration have been considered, there appears to have been no or little consideration of the use of large denomination bank notes, possible abuse of cash intensive businesses, use of prepaid cards, handling of cash by TCSPs, or reasons for transporting cash cross-border. This may be due in part to Liechtenstein's monetary and customs unions with Switzerland, whereby Liechtenstein's border with Austria is monitored by the Swiss Border Guard Corps and there are no border controls between Switzerland and Liechtenstein. In general terms, the AT considers that there is a need to update the analysis of ML risk presented by the use of cash and prepaid cards e.g., by analysing: (i) economic sectors presenting greater exposure to the use of cash and reasons; (ii) recurrence of use of cash above a certain threshold; and (iii) trends on the use of cash as identified through SARs/STRs and analysis by the FIU.

126. Finally, the use of shell companies has been identified as a high inherent risk in NRA II, and an amendment in 2019 to the CC (Art. 165) to include tax savings as asset components subject to ML has largely curtailed their use in the private sector. However, the authorities could not quantify the extent of this change, e.g., number of business relationships that had been terminated with shell companies and had not analysed fund outflows after relationships had been closed, e.g., value and destination. Accordingly, understanding of how residual risk has changed in this area is rather limited.

Country's understanding of TF risk

127. For many countries, the process for identifying, assessing, and understanding TF risk primarily involves analysing terrorist activities conducted within, or which are linked to, the jurisdiction, and examining the financial needs of those involved. The demographic and geographical factors applicable to Liechtenstein are such, however, that domestic terrorism risk is very low. Liechtenstein has not experienced any terrorist attacks to date and the likelihood that it will become a target of terrorism is low. No terrorist organisations are operating or are present in Liechtenstein and there are no parts of its population that would be sympathetic to terrorist causes.

128. As an IFC, the country recognises that it is more likely that its exposure to TF arises from high levels of cross-border business and financial transactions and activities, with the attendant possibility of services and products offered, or assets channelled through Liechtenstein, being used by parties outside the country to fund terrorism abroad. In line with this, important information on funds transfers for banks and MSBs to, and from, Liechtenstein has been collected by the FMA to promote a better national understanding of cross-border threats, and the authorities have also used ML data in order to identify possible TF elements, e.g., SARs/STRs involving higher risk countries. Overall, residual TF risk is assessed by the country as medium for FIs and DNFBPs, and TF threat is almost exclusively determined as emanating from incoming/outgoing fund flows from, and to, higher risk countries. For VASPs, the residual risk is medium-high. This and related NRA analyses demonstrate a good broad understanding of core risk by the country.

Gaps in understanding of TF risk

129. The country's understanding of risk is affected by not having a full understanding of transactional links to countries presenting a higher TF risk and use of ATMs in countries that neighbour conflict zones (see below).

130. As explained above, the authorities have analysed inflows and outflows of funds on a country-by-country basis. However, the analysis of why funds are received from, and sent to, countries presenting a higher TF risk is rather general and does not explain the reason for, and nature of, such links. This point is considered further above (ML risk) and is considered to have only a minor effect on TF risk understanding, given that there are no indicators that the country is being used to finance terrorism (distinct from ML).

131. Whilst risks posed by cash couriers and by the cross-border movement of cash are considered in the TF analysis, the authorities have not considered the risk that cash withdrawals may be made from accounts held at Liechtenstein banks through ATMs in countries that neighbour conflict zones (including through prepaid cards) as this information is not available (though this is set by the authorities as a risk indicator to be considered by the private sector). For the reasons given above, this is considered to have only a minor effect on risk understanding.

2.2.2. National policies to address identified ML/TF risks

132. There is strong political commitment to AML/CFT, the work of the PROTEGE WG and work of the authorities. There is a close and positive relationship between the PROTEGE WG and the government. Liechtenstein has produced: (i) a Financial Centre Strategy (updated in 2019); (ii) an AML/CFT Strategy, which includes four strategic objectives; (iii) a national Action Plan formulated through the PROTEGE WG; and (iv) a policy covering asset recovery.

133. With one exception (explained below), national policies and activities successfully address risks that have been identified in risk assessments. Shortcomings identified above in risk understanding have a cascading effect in that they have not been addressed through policies or activities.

134. Liechtenstein has adopted an integrated Financial Centre Strategy, aimed at strengthening the country's attractiveness as an innovative IFC for the long term, while ensuring greater transparency and compliance in the AML/CFT field. One of the objectives of the strategy is for the Government and authorities to take effective and consistent action against the abuse of the financial centre for the purpose of ML/TF. Another is trust in the integrity of the financial centre.

135. The AML/CFT Strategy was adopted by the PROTEGE WG in June 2020, taking account of all risk assessments conducted, and endorsed by the Government in July 2020. The strategy was updated in February 2021 and endorsed by the Government in July 2021. The Strategy looks to reinforce preventative and repressive actions and calls for: (i) effective implementation of international obligations and standards to combat ML/TF; (ii) a risk-based focus on increasing effectiveness in combatting ML/TF and improving risk management in the private sector; (iii) effective prosecution of ML and TF; and (iv) further intensification of national and international cooperation, coordination, and exchange of information. The PROTEGE WG is in charge of implementing the AML/CFT Strategy and has to report annually to the Government and provide advice for strengthening the AML/CFT system.

136. The PROTEGE WG has also developed a national Action Plan (first produced in 2018), based on the findings of NRA I and II, which includes deadlines (until the end of 2022) and one responsible authority for completing each identified action. Actions are appropriate and well-shaped for risk mitigation purposes and are linked clearly to the FATF Recommendations and risk assessments. Examples of ongoing and implemented actions have included: (i) collection of a more comprehensive set of customer data to support analysis of risk, including countries of origin of BO, geographical exposure, and types of products and services offered; and (ii) for VASPs - regulation, introduction of a specific supervisory risk model at the FMA, mandatory use of chain analysis tools and exclusion of application of simplified CDD (SDD) measures by VASPs. However, the plan does not include any explicit action to examine and estimate the extent of use of Liechtenstein's financial sector to launder the proceeds of foreign tax offences. The national Action Plan has been updated six times since 2019 – the most recent update being in August 2021. Implementation of the national Action Plan is monitored by the chair of the PROTEGE WG on a monthly basis.

137. With regard to TF, the national Action Plan has included annual data collection relating to inflows and outflows, further specialisation and strengthening of capacities of OPP and in the National Police, and issuance of guidance to the private sector on business-wide risk assessments.

138. Resourcing reforms have been driven by the national Action Plan to a lesser extent since budgeting is handled at authority level. It is unclear whether there is a coherent macro-level process for monitoring the allocation of resources on an ongoing basis taking account of risks and information in NRA II. This is the case, for example, for resources needed to respond to regulation of the VASP sector and to support activity in the investigation and prosecution of serious tax offences.

139. The PROTEGE WG has adopted an Asset Recovery Policy, which was endorsed by the Government in November 2020. It pursues a global approach to be followed by all competent authorities (law enforcement authorities (LEAs), FIU, the judiciary) aimed at depriving criminals of any material benefit from their crimes by aggressively tracing, seizing, and confiscating property.

140. While the AT recognises the value of all the strategic and operational documents outlined above, the authorities would still benefit from a set of formally documented high-level national policies pitched between strategic objectives and detailed actions - to guide competent authorities in the delivery of their statutory functions (such as for confiscation). Such policies might cover: (i) products and services, or parts of the world, that do not align with the country's risk appetite; (ii) handling of financial intelligence, e.g., prioritisation of typologies linked to overall risk profile of the country; and (iii) supervisory objectives.

2.2.3. Exemptions, enhanced and simplified measures

141. Cases triggering the application of EDD (requirements and factors to consider) and simplified measures (factors to consider) are consistent with risks identified in NRA II. However, there are some exemptions from the application of preventive measures which have not been supported by risk assessments at country level. In the context of an IFC, one exemption has a significant impact on the application of CDD (see below).

142. In addition to areas covered in the FATF Recommendations, FIs, DNFBPs and VASPs are all required to apply EDD measures to: (i) relationships with customers linked to states with strategic deficiencies; (ii) complex customers; and (iii) transactions that have no apparent financial purpose or understandable lawful purpose (conducted for example through shell companies). Regarding higher risk countries (ML/TF), the FMA has also published a list of more than 120 countries that automatically present an increased geographic risk (countries identified by credible sources as having significant levels of corruption or other illicit activities). This list is attached to FMA Guideline 2013/1 on the risk-based approach (List A). The FMA states that EDD measures must be applied at the latest when a business relationship is linked to countries with increased geographical risk and another risk factor (e.g., high volume of assets or transactions) comes into play. This is consistent with Liechtenstein's position as an IFC that focusses on wealth management.

143. In addition, there is a general requirement to collect information on source of wealth (SoW) and source of funds (SoF) for all customers, which is consistent with risks identified for wealth management and which incorporates risk-based elements. Other factors identified in NRA II must also be considered as risk-increasing factors, e.g., signatory rights and powers of attorney to external third parties and life insurance products with higher single premia (FMA Guideline 2013/1).

144. Based on NRA-VA, a number of EDD requirements are in place including: (i) very low thresholds for CDD conducted by VASPs; (ii) prohibition on SDD procedures; and (iii) absence of a threshold to conduct CDD when carrying out occasional transactions.

145. A summary of exemptions from application of the DDA that are not supported by a risk assessment at country level are set out at c.1.6 in the TC Annex. With one exception, it is unlikely that they will have a significant impact on the effective application in Liechtenstein of preventive

measures. However, an important and widely used exemption is applied by investment funds (and indirectly by asset managers) in respect of underlying customers of banks that invest in non-private investment funds. Subject to an assessment of risk of each bank, the investment fund is not required to find out the identity of the bank's underlying customer(s). The application of the scope of this exemption to private investment funds has recently been further narrowed, in line with NRA II-ML. This exemption is commonly found in other countries (including throughout the EEA which follows risk factor guidelines issued by the European Banking Authority) and can be accommodated under R.1 and other international standards, but no risk assessment has been conducted at country level to support its use in Liechtenstein.

146. An exemption is in place also for bank accounts operated by lawyers, where the bank is not required to find out the identity of the lawyer's underlying customer, so long as it receives a declaration from the lawyer that transactions through the account relate to a set of prescribed lower risk transactions or proceedings before a court. In this case, the AT has not seen an assessment to support use of the concession. Accordingly, the AT has limited grounds to evaluate whether or not the exemption is supported by a proven low risk.

2.2.4. Objectives and activities of competent authorities

147. Objectives and activities of the competent authorities are commensurate with risks identified in NRA II and policies.

148. The national Action Plan is used in a way that ensures that the objectives and activities of the competent authorities (and one SRB) are consistent with the ML/TF risks identified. This supports a statutory requirement placed on these authorities to consider NRA findings when prioritising their activities (and to do so in a risk-based manner). In particular, the plan has supported a restructuring of the FMA, appointment of two specialised public prosecutors, and led to an increase in personnel resources at the National Police. The national Action Plan is also presented to the Government, which meets regularly with competent authorities, e.g., monthly with the FIU.

149. The supervisory system in Liechtenstein was completely redesigned in 2018/19 and risk-based approach strengthened. This has facilitated recent supervisory efforts in respect of: (i) the assessment and verification by FIs, DNFBPs and VASPs of SoW and SoF; (ii) business risk assessments; and (iii) reporting of suspicion. These efforts were directly linked to findings in NRA II and appear to have had some success, since understanding of risk and the application of AML/CFT preventive measures are now generally good in the banking and TCSP sectors (see Chapter 5). The FMA has also re-focused its efforts on the use of shell companies and life assurance premia in response to risks identified in NRA II.

150. The OPP and the National Police have a high awareness of the need to consistently pursue and investigate all ML-related activities. This awareness has materialised in the significant number of ML investigations initiated so far (see IO.7). On the other hand, the methodology used to develop NRA II focussed on cases/ML activity investigated and prosecuted in Liechtenstein and as already noted, an overarching threat assessment has not been conducted.

151. In line with the policy covering asset recovery, LEAs consider seizure and confiscation as a priority action when investigating proceeds-generating offences. Both conviction and non-conviction-based confiscation are frequently applied in practice. The outcome of the authorities'

activities, both in terms of assets seized and confiscated, is generally in line with the country's risk profile.

152. In line with the AML/CFT Strategy, the FIU and National Police have developed specific documents and instructions on how to investigate TF.

2.2.5. National coordination and cooperation

153. Cooperation and coordination among stakeholders are effective and one of the strengths of the jurisdiction. The country applies a "whole of government approach" – whereby there is close and effective cooperation in the development and implementation of policies and activities between competent authorities through the PROTEGE WG and other groups. Efforts in this regard are a political objective - constituting a pillar of the AML/CFT Strategy – and resources are adequate.

154. The PROTEGE WG, established in 2013, is the permanent cooperation mechanism used to coordinate the development and implementation of policies, and oversee activities in the AML/CFT field. Permanent members of the PROTEGE WG include the Ministry for General Government Affairs and Finance, the FMA, the FIU, the OPP, the Court of Justice, the National Police, the Office of Justice, the Office for Foreign Affairs, and the Fiscal Authority, all of which are represented at a senior level. The Chamber of Lawyers (SRB) is invited to attend meetings, when appropriate to do so. The group is led by the Ministry for General Government Affairs and Finance, has its own secretariat, and its head is directly under the authority of the Prime Minister and Finance Minister. It reports regularly and directly to the Government.

155. The PROTEGE WG, which meets on a frequent basis (almost once a month during 2020 and 2021), has led discussion on deficiencies identified in Liechtenstein's AML/CFT framework and on measures to address gaps, e.g., discussion on the expansion of predicate offences with regard to serious tax offences, deficiencies in the DDA, and transition to risk-based supervision at the FMA.

156. The AT reviewed the agenda for all of the PROTEGE WG meetings held since 2019, along with a summary provided of key discussions and decisions. Based on this information, it is clear that the WG acts as an effective forum for coordinating risk assessments, identifying changes to international and EU standards (and consequential legislative amendments), and preparation for external assessments. It is less clear from the material provided whether the WG has a more strategic policy development role.

157. Alongside the PROTEGE WG, there are three operational sub-groups which have similar membership. One sub-group is led by the OPP, and this discusses ongoing criminal investigations and prosecutions. The group has met on almost a monthly basis in 2020 and 2021 following meetings of the PROTEGE WG. More frequent meetings are held on an ad hoc basis as needed. This group has discussed TF issues, including cases described in Chapter 4 (IO.9) and some TF typologies connected to VASPs. Another sub-group is led by the FMA and discusses industry compliance (e.g., levels of reporting), supervision, and enforcement cases. This sub-group meets on a bi-monthly basis and has met 10 times in 2020 and 2021 (to August). It focuses primarily on ML/TF cases as well as risks and typologies. These meetings play a key role in the FMA's application of risk-based supervision, and so are attended also by prudential supervisors. Both groups also discuss new business developments, changes in behaviour etc. A third sub-group

covers TFS and is led by the Office for Foreign Affairs. The group has met on four occasions in 2020 and 2021 (up to August) in addition to regular consultation on implementation of EU sanctions and amendments to domestic legislation. Membership of this third sub-group also includes the Diplomatic Representation in Brussels and Government Legal Services.

158. The three sub-groups operate independently of the PROTEGE WG and are not accountable to it. Nevertheless, reports are presented, by way of background, at each WG meeting by the sub-groups.

159. The remit of PROTEGE WG discussions extend, as necessary, to financing of proliferation of weapons (PF). However, discussion on PF have focussed on: (i) implementation of TFS, without distinguishing between TF and PF; and (ii) licensing of imports and exports (that are relevant for PF purposes), where the Office for Foreign Affairs and the FIU have regular direct contact with the Swiss State Secretariat for Economic Affairs (SECO) which has responsibility for licensing imports and exports for Switzerland. There has not been a more general discussion of PF policies and activities.

2.2.6. Private sector's awareness of risks

160. Almost universally, the private sector agrees with residual sectoral risks in the NRA-ML and demonstrated good familiarity with NRA II and its findings.

161. Advanced drafts of NRA II were shared with the private sector through their respective professional associations in quarter 2, 2020. This was followed by an online presentation on NRA II in May 2020 and all sectors were subsequently invited to identify substantial mistakes. Final NRA documents were also circulated through these associations in July 2020 and also sent directly to FIs, DNFBPs and VASPs not parts of such associations.

162. An executive summary of NRA II (Core Elements of the NRA of the Liechtenstein Financial Centre with respect to ML and TF) was sent to associations and all market participants in February 2021 and is also sent to all new market participants by the FMA and Chamber of Lawyers.

Overall conclusions on IO.1

163. Liechtenstein has demonstrated a strong and high-level political commitment to fighting ML/TF supported by necessary strategies, action plans, cooperation, and coordination. As a result, it has a good broad and convergent understanding of core ML/TF risks, including for the two sectors weighted as most important (banking and TCSPs) and the objectives and activities of competent authorities are commensurate with risks.

164. As explained above, some threats have not been fully examined and some inherent ML risks not considered, which means that all risks are not fully understood. This is particularly so for ML, where risks are considered by the AT to be greater. In considering the rating, the AT has focussed on two areas where there is a need for improvement, and which are relevant to sectors weighted most important. The first concerns information held in respect of the TCSP sector - where valuable information held by the authorities does not include data on the types and location of non-bankable assets administered in the country. The second concerns estimation of the threat that is presented by laundering of the proceeds of tax offences committed abroad. Whilst the authorities recognise the threat, have taken important action to address vulnerabilities

and believe that the extent of ML is limited, they have not examined or estimated the extent of the threat.

165. In the view of the AT, these and other gaps identified in understanding of risk, call for moderate improvements to be made to support an otherwise good broad understanding of risk. The AT has particularly taken into account: (i) action taken by the authorities since 2009 to implement international tax transparency standards - that has had some positive effect on reducing ML/TF risk in Liechtenstein - and to provide administrative assistance whenever MLA requests solely concern tax evasion; and (ii) the significant efforts employed to collect a broader set of data for analysis under NRA II.

166. The AT is of the view that IO.1 is achieved to a large extent. **Liechtenstein is rated as having a substantial level of effectiveness for IO.1.**

3. LEGAL SYSTEM AND OPERATIONAL ISSUES

3.1. Key Findings and Recommended Actions

Key Findings

Immediate Outcome 6

a) Liechtenstein FIU constitutes an important source of financial intelligence in the overall AML/CFT system of the country. Financial intelligence it produced is considered to be of a high quality by its primary users - prosecutors and LEAs. Whilst the majority of ML investigations are triggered by sources other than the FIU's analytical reports – primarily by MLAs/information received by foreign counterparts, the FIU's analyses are an inevitable part of any investigation/operational activity carried out by LEAs. Overall, financial intelligence has been widely used in investigations and evidence gathering in ML and confiscation cases.

b) Although the FIU expressed a general satisfaction with the quality of SARs/STRs received, some areas still warrant improvements, including the following: (i) although the SARs/STRs filed by persons subject to the DDA are generally commensurate with the landscape of prevalent proceeds-generating crimes in the country, they have rarely targeted some of the higher risk predicate offences, e.g., tax offences; (ii) increase in the overall number of SARs/STRs in recent years did not trigger tangible difference in number of the FIU's disseminations to LEAs; (iii) tendency of reactive or non-reporting, which was prevalent before 2018, can still be observed, although to a lesser extent.

c) During the period under review 7 TF related SARs/STRs were filed. Whereas this number may appear low, the AT did not observe that persons subject to the DDA were not vigilant in exercising their duties with regard to TF related suspicious transactions reporting.

d) The FIU has so far produced several comprehensive strategic analysis reports mostly based on trends and methods explored by the Egmont Group. Whilst this is to be commended, the country would further benefit from strategic analysis in relation to (i) TF-related typologies that would tackle the risks identified in the NRA-TF – i.e., flows to and from high-risk jurisdictions, and (ii) typologies and/or red flags related to laundering of proceeds of foreign tax crimes; (iii) appropriateness of SAR/STR reporting in relation to the issues specified above.

d) The FIU's necessary infrastructure (IT security and data storage) is in place. On the other hand, the growing workload and recently initiated cases with complex and long-lasting financial intelligence analysis require adequate resources and can hardly be managed if the current number of staff does not increase.

e) The size of the jurisdiction allows prompt information exchange and consultations among competent authorities. Interviews and statistical data on number of information requests sent by LEAs to the FIU, together with the case examples presented, confirm that there is extensive inter-agency cooperation and information exchange, while some formalistic issues in relation to cooperation with Fiscal Authority were solved with the legislative amendments in April

2021. No issues concerning the FIU's operational independence and confidentiality of information were identified.

Immediate Outcome 7

a) Liechtenstein's legal and institutional framework enables effective investigation and prosecution of all types of ML. Whilst the FIU, law enforcement and prosecution authorities have high awareness of a need to consistently pursue and investigate all ML-related activities, the AT is of the view that, given the context of an IFC, there is a lack of ML investigations/prosecutions targeting sophisticated ML schemes which potentially include complex legal structures established and managed in Liechtenstein.

b) Competent authorities routinely detect, investigate, and prosecute ML whenever they come across evidence that a predicate offence has been committed. Given that the vast majority of predicate offences have been committed abroad, ML investigations are mostly triggered by incoming MLA requests. Cases presented to the AT confirmed that the FIU and its analysis of financial flows are essential and inevitable parts of any ML investigation carried out in Liechtenstein.

c) The methodology used to develop the NRA includes the analysis of existing cases/ML activity investigated and prosecuted in Liechtenstein. In view of that, the risks and threats identified in the NRA mirror the typologies already observed in the country. Consequently, consistency between the types of ML activity being investigated and prosecuted with the country's threats and risk profile and national AML/CFT policies has been attained, with the exception on threats posed by tax crimes committed abroad. This type of criminality has never been subject to a ML prosecution in Liechtenstein. Whilst the assessors are aware that a precondition for success of such investigation is obtaining information from a foreign counterpart on specific tax crime(s), it appears that both LEAs and prosecutors would need to gain further experience to deal with such cases.

d) Liechtenstein's judiciary has achieved convictions for all (three) types of ML cases: of the 2 types of ML, the self-laundering of the proceeds of fraud committed abroad is still a prevailing typology and 3rd-party laundering is encountered infrequently as are autonomous ML prosecutions, although the competent authorities demonstrated a good understanding of what constitutes these different types of ML cases. The judiciary is able to draw inferences based on objective, factual circumstances and obtain a conviction for ML in absence of a conviction for predicate offence(s). Objective, factual circumstances may also serve as a basis to establish the perpetrator's means rea with regard to the origin of proceeds (i.e., knowledge that the proceeds were of a criminal origin).

e) The vast majority of convictions for self-laundering in Liechtenstein were achieved after the trials for predicate offences were completed abroad. When determining the sentences in these cases, the judiciary took into account sentences already pronounced for these predicates. Consequently, sanctions in these ML cases amounted to several months of imprisonment or were suspended sentences. The AT does not find them sufficiently dissuasive and proportionate. For cases of stand-alone and autonomous ML, as well as for those where legal persons were convicted, the AT is of the opinion that sanctions imposed are rather minimal.

f) Liechtenstein introduced and has applied in practice criminal justice measures where, for justifiable reasons, ML conviction cannot be secured. These measures include (i) non-conviction-based confiscation (Art. 356 CPC) and (ii) criminalisation of failure to report a suspicious transaction by a reporting entity (Art. 30 (1a) DDA).

Immediate Outcome 8

a) Confiscation of the proceeds of crime is pursued as a policy objective in Liechtenstein. This has not only been confirmed through different strategic and policy documents but also through introduction of a comprehensive legal framework and continuous strengthening of the capacities of LEAs and prosecutors aimed at better detecting, seizing/freezing, and confiscating the proceeds of crime.

b) LEAs and prosecutors consider seizure and confiscation as a priority action when investigating any proceed generating offence(s). Financial investigations are routinely applied and communication between different authorities appears to be smooth and fruitful in each phase of the seizure/confiscation proceedings. Judicial authorities are also vigilant and aware that proceeds may dissipate instantly and thus consider a grounded suspicion as sufficient to approve freezing orders (both for proceeds and instrumentalities of crime) over the course of a criminal investigation. Both conviction and non-conviction-based confiscation, including the confiscation of equivalent value, are frequently applied in practice.

c) In general, the authorities actively seek and provide assistance from/to their foreign counterparts when seeking/tracing proceeds of crime. Freezing/seizing orders in the course of a criminal investigation granted by Liechtenstein's courts are often accompanied with a corresponding MLA request to foreign counterparts. These requests usually ask for further details/evidence on predicate offence(s). However, a lack of responses from some foreign jurisdictions to these MLA requests (responsibility for which exclusively lays with these countries) may hamper the country's ability to effectively confiscate proceeds of crime.

d) Liechtenstein has a framework treaty with Switzerland which stipulates that the execution of cross border controls is delegated to the Swiss Border Guard Corps. Statistics and discussions held with the Swiss Border Guard Corps revealed certain weaknesses in the system. These considerations were also discussed in the mutual evaluation report of Switzerland. However, the AT observed that the communication between the Swiss Border Guard Corps and the National Police is intensive and smooth. Any infringement identified by Swiss Border Guard Corps is immediately notified to the National Police.

e) The outcome of the authorities' actions, both in terms of assets seized and confiscated, is generally in line with the country's risk profile. Whilst the confiscation results do reflect the assessment of ML/TF risks, the corresponding findings expressed under IO.7 (lack of prosecutions related to tax crimes) are also valid when discussing the effectiveness of the confiscation system.

Recommended Actions

Immediate Outcome 6

a) The authorities should carry out further review/analysis with regard to:

- (i) SAR/STR reporting on high-risk predicates, i.e., laundering of foreign tax offences proceeds; and

- (ii) TF related SAR/STR reporting taking into account transactions with TF related high risk jurisdictions. Both analyses should be reviewed periodically, possibly through the public-private partnership platform.

b) The FIU should develop indicators/red flags for the private sector which would assist them in reporting suspicious transactions which may potentially include proceeds of foreign tax offences. These indicators should be developed through usage of existing typologies observed in IFCs worldwide where the laundering of tax offences' proceeds was identified as a high risk. The expertise of the FIU on this particular matter should be further strengthened also through the examination of these typologies and developing guidance for analysts on how such typologies could materialise in Liechtenstein.

c) The authorities should consider developing TF-related typologies (which would include use of cash) based on the risks identified under the NRA-TF.

d) The FIU human resources should be revisited taking into account the amount of work it is currently assigned with. In the view of the growing number of VASP related SARs/STRs, the FIU should consider recruiting staff with experience in this field.

Immediate Outcome 7

a) Liechtenstein authorities should ensure that the OPP, investigative judges, the National Police and the FIU effectively target complex, large-scale ML, including cases involving funds deriving from high-risk predicates committed abroad (corruption, tax crimes, trafficking in narcotic drugs, etc.), which were then layered through Liechtenstein FIs, DNFBPs or VASPs. To achieve this objective the authorities should set out the range of circumstances to address the position where complex legal structures are abused for ML.

b) Competent authorities should continue to prioritise investigations related to the financial component of predicate offence and improve their understanding of typologies related to the main risks the jurisdiction is facing (cases involving e.g., TCSPs, who may have acted as professional intermediaries and concealed or made arrangements in respect of criminal property or failed to report their knowledge or suspicion of ML).

c) Liechtenstein should consider increasing the resources of the OPP, the FIU and the National Police to add a number of experienced staff in each of these institutions. Inclusion of more forensic accountancy resources to enable undertaking in complex ML investigations and prosecutions should also be considered.

d) Consideration should be given to the criminalisation of simple tax evasion where income is not declared or not fully declared in the tax return, so that this constitutes a predicate offence to ML.

e) Judicial authorities should take steps to make sentences for ML proportionate and dissuasive. The courts need to develop a greater understanding of the need for a sanctioning regime which would ensure that dissuasive sanctions are applied against both, natural and legal persons.

Immediate Outcome 8

a) The authorities should strengthen and streamline the application of the extended confiscation mechanism through specific guidelines and trainings for the OPP, investigative judges and the National Police.

b) The authorities should strengthen the cross-border control through: (i) joint threats analysis with Swiss and Austrian cross border authorities, with such analysis providing the basis for better identification and investigation of ML/FT suspicions; (ii) provision of intelligence and/or information to the customs authority of Switzerland in order to enable them to identify targets for control, and suspected passengers, cargo and mail; (iii) developing a guideline for the National Police for detecting cash smugglers which would include indicators for profiling those involved in such activity; and (iv) putting in place measures to mitigate the risks stemming from the lack of a declaration/disclosure system between Switzerland and Liechtenstein.

167. The relevant IOs considered and assessed in this chapter are IO.6-8. The Recommendations relevant for the assessment of effectiveness under this section are R R.1, R. 3, R.4 and R.29-32 and elements of R.2, 8, 9, 15, 30, 31, 34, 37, 38, 39 and 40.

3.2. Immediate Outcome 6 (Financial Intelligence ML/TF)

3.2.1. Use of financial intelligence and other information

Access to information

168. Liechtenstein LEAs and prosecutors have access to and in practice make systematic use of a wide variety of sources of financial intelligence and other relevant information when investigating ML and predicate offences, tracing assets and identifying criminal money flows. Parallel financial investigation is an integral part of investigations of proceeds generating crimes.

169. The Liechtenstein FIU constitutes an important source of financial intelligence. The FIU is the central authority for the receipt and analysis of SARs/STRs. These SARs/STRs, together with the information received from abroad (directly or through National Police/OPP) are a primary source for the FIU to produce financial intelligence. During its analysis, the FIU communicates intensively with persons subject to the DDA – it is empowered by the law, since 2016, to request information from them even in absence of an SAR/STR being submitted beforehand. At that, accessing information held by persons subject to the DDA is now part of the FIU's routine activities (see core issue 6.2).

170. The FIU has direct access to the several databases: list of licensed/persons subject to the DDA, Liechtenstein central person register, Commercial database on legal entities, Central Vehicle register and Court register, which is publicly available. The FIU has also direct access to some databases that include adverse media information on individuals and organizations. BO and bank accounts register databases have been directly available to the FIU since 1 October 2021.

171. Other types of information (information on landowners, export/import into/out from Liechtenstein through Switzerland, general law enforcement information and tax information)

are obtained by the FIU indirectly through the requests to respective authorities. Details on the databases accessible to the FIU are provided below.

Table 3.1: List of FIU databases

Database		Access modality	Content
FMA list of licensed/registered persons subject to the DDA		Direct, open-source (website)	List of all registered persons subject to the DDA/license holders.
ZSD – Central Person Register		Direct	Natural persons: Information on any person living and/or working in Liechtenstein, family relations, employer information, information regarding directorships for Liechtenstein legal entities, type of work permit (for foreigners) etc. Legal persons: General information, information on legal representatives
Commercial register		Direct	Information on legal entities/arrangements incorporated in Liechtenstein, including the purpose, dates of changes, directors/representatives, address of administrating TCSP etc.
BO register (live since 1.8.2021, fully operational as of 1.10.2021)		Direct	Information on BOs of legal entities and legal arrangements in Liechtenstein.
Account register (live as per 1.10.2021)		Direct	Information on opened/closed accounts, type of account, contracting party, BO, persons with proxy rights
Central vehicle register		Direct	General information on all vehicles matriculated in Liechtenstein (holder, other vehicles held, vehicles held previously etc.)
Land register		Indirect	Information on landowners
Office for Economic Affairs – Import/Export statistics		Indirect	Information on services imported/exported into/out of Liechtenstein through Switzerland
Police database (general and international		Indirect	General law enforcement information on natural and legal persons/arrangements, involvement of such in international cooperation queries etc.

cooperation information)			
Court decisions		Direct, open-source (website)	Court decision (anonymized)
Tax authority		Indirect	Tax information and enforcement information on natural and legal persons
Refinitiv World-Check		Direct	Adverse information on individuals, companies and organisations worldwide
LexisNexis		Direct	Media content from a large variety of publications in a large number of languages world-wide
D & B Factiva		Direct	Media content from a large variety of publications in a large number of languages world-wide, company information from open sources

172. Most of the financial intelligence and related information used by LEAs/prosecutors is obtained via the FIU, before or during their ML investigations. This also includes foreign intelligence provided spontaneously or upon request by its counterpart FIUs (see IO.2). Detailed information on cooperation between the FIU and other national authorities, including the number of requests, is provided under section 3.2.4 (cooperation and exchange of information/financial intelligence).

173. The FIU is also empowered to request information from competent domestic authorities and LEAs, including documents related to findings of supervisory activities and data related to ongoing investigations (see core issue 6.4). As regards the methods of making financial intelligence available for competent authorities, this is done either through analytical reports disseminated by the FIU spontaneously, or through requests from competent authorities (see core issue 6.3). The FIU disseminates reports to a number of institutions, including LEAs, prosecutors and supervisory agencies. The reports submitted to the supervisory authorities are aimed at further enhancing the effectiveness of supervision over different categories of entities, usually highlighting specific issues upon which greater focus should be paid.

174. LEAs and prosecutors also use other relevant platforms, such as the CARIN network and a network of liaison officers to obtain information which would help them in on-going investigations when seeking ML/TF/predicate offence related evidence or tracing assets. While carrying out a financial investigation, competent authorities collect information and data from different sources/databases.

175. The National Police has access to a wide range of national and international databases of information to conduct investigations. Direct information sources include list of databases, part of which are the same that the FIU has access to. The additional direct sources of the National Police include, but are not limited to the National Fingerprint Database, Driver's license Database, information on people who are staying in a hotel in Liechtenstein, information on stolen documents and motor vehicles, criminal records of persons etc. From the foreign databases, the

National Police has access to Interpol, Europol, Liaison Officer network, CARIN network. The National Police is also involved in several projects of Interpol and Europol and is able to receive information this way.

176. The National Police is also able to seize banking documents based on a warrant by an investigative judge. These documents are obtained in paper form, which might create technical difficulties when conducting financial investigation. In the Action Plan of PROTEGE WG there is a measure is foreseen to enable transmission of electronic transaction data to the National Police. Authorities advised that implementation of this measure is still in the stage of discussions.

Use of financial intelligence and other information

177. There are three main triggers for initiating investigations on ML. These are: (i) incoming MLA requests, including spontaneous information received from abroad, (ii) financial intelligence reports submitted by the FIU, as well as (iii) information obtained by the National Police in course of their activities/financial investigations. Other triggers are the individual complaints of injured parties, media articles and any other information that may indicate that ML/TF/predicate offence was committed. Findings from the activities of supervisory authorities (especially the FMA) and the Fiscal Authority can also trigger a ML investigation, though so far it has not been a common practice.

178. Financial investigations are carried out routinely for vast majority of predicate offences – for all those which include proceeds generating elements. Depending on the way cases are triggered, either the National Police, the OPP or the investigative judge initiate investigations (see IO.7 for details). In all cases where there are financial components, these authorities consider whether there are elements of ML and then actively engage the FIU in these analyses.

179. As a matter of procedural provisions in the country, analytical reports by the FIU are transmitted to the OPP for the purposes of investigation. Further to a submission of an analytical report, the interaction between the FIU and the OPP is extensive. As a matter of practice, prior to submitting a report to the OPP, consultations are carried out between the two institutions to better understand and analyse ML/TF/predicate offence suspicion. The National Police also take part in these consultations as they are responsible for execution of investigative actions.

180. Financial intelligence produced by the FIU is considered to be of a high quality by its primary users - prosecutors and LEAs. Statistics and cases presented by the authorities clearly indicate that the FIU analysis is not a major trigger point for ML investigations - ML/predicate offence investigations mostly result from information the OPP receives from incoming MLAs requests or from different informal information exchange by the National Police. Vast majority of the predicate offences to ML are committed in foreign jurisdictions, this being the main reason why MLA requests/information received from abroad are the most important source of financial intelligence and thus ML/predicate offence related investigations. If, for example, there is a suspicion of ML identified by the OPP from an MLA request, the OPP initiates investigations into ML ex officio. Once an MLA and documents seized under MLA proceedings indicate that a predicate offence proceeds have links with Liechtenstein FIs, DNFBPs, VASPs or physical or legal person residing in the jurisdiction, the OPP, ex officio, launches an investigation into ML and immediately engages the FIU into it. Relevant information is shared with the FIU which then acts as a main facilitator of financial intelligence analysis. If in the course of investigation information such as whether or not a business relationship exists with persons subject to the DDA, who is a

BO of a legal person/arrangement, details on money flows, etc. this information is obtained via the FIU. If it might serve as evidence in the court proceedings, a justified request would then be sent to the court requiring its approval to obtain the information directly from persons subject to the DDA.

181. The table below indicates the number of ML investigations, initiated by different authorities/sources followed by indictments and convictions. The statistics provided do not clearly distinguish the initial source (e.g., whether it was an MLA, SAR/STR or other trigger) of ML related investigations. As noted above, whenever there is an MLA request which indicates potential ML/TF/predicate offence links to Liechtenstein, this information is shared with the FIU. For this reason, a number of investigations which were (essentially) triggered by an incoming MLA are, in majority of cases, categorised as those initiated by the FIU's analytical report. Whilst formally speaking this may be right, the table provided below indicates number of investigations and indictments where this approach has materialized.

Table 3.2: Triggers of ML Investigations

Year	**Investigations**					**Indictments**	**Convictions**	**Acquittals**
	Cases	FIU	Police	OPP (MLA)	Complaints			
2016	**89**	55	13	14	7	7	5	1
2017	**86**	45	21	17	3	20	8	0
2018	**77**	44	15	15	3	12	8	1
2019	**87**	43	28	10	6	20	14	0
2020	**121**	50	36	20	15	12	13	2

182. Altogether, statistics provided above, in conjunction with the cases presented to the AT (some of which are presented in case boxes below, as well as in IO.7) demonstrate that financial intelligence has been widely used in investigations and evidence gathering in ML and confiscation cases. Given the jurisdiction's risk and context, the AT finds it important that the incoming MLAs/ information received from abroad are extensively used and explored for ML related investigations. On the other hand, the AT also observed lack of cases and thus insufficient use of financial intelligence in pursuing the laundering of proceeds of tax offences committed abroad. As also observed under IO.7, the role of the FIU in this particular area needs to be strengthened given the fact that by a virtue of its competences, access to information and communication it has with persons subject to the DDA, it is the best positioned, among competent authorities, to signal suspicious money flows which potentially include proceeds of foreign tax offences. One of the ways in how this could be addressed is to further develop indicators/red flags for the private sector based on typologies observed in IFCs worldwide where the laundering of tax offences proceeds was identified as a high risk. In parallel, the expertise of the FIU on this particular matter should be further strengthened through the examination of these typologies and developing guidance for analysts on how such typologies could materialise in Liechtenstein.

183. No separate statistics are available on the number of investigations on predicate offences. These are either investigated abroad (as the vast majority of predicate offences are committed outside the jurisdiction), while if committed in the country, competent authorities would investigate both, predicate offence and ML. This approach appears to be largely in line with the risks and context of the jurisdiction.

Box 1

Financial intelligence generated by the FIU and used to initiate an investigation

Case 1: Investigations for fraud were initiated in Germany against a German citizen. He was also attributed to the Swiss company. The suspect received assets of around EUR 20 million from this company in Liechtenstein, which were subsequently invested in another company. There was a suspicion that these assets came from the above-mentioned fraud committed in Germany. An initial report was made by the Liechtenstein FMA to the OPP. At the same time, the FIU investigated the matter through its partner authorities, which resulted in a detailed report to the OPP. The suspects are several German nationals and the company in Liechtenstein. The OPP and the National Police launched investigation on the basis of the information and documents submitted by the FIU. In particular, the origin of assets (fraud committed in Germany) could be traced on the basis of the FIU information. Several coercive measures were applied upon approval of the investigating judge. Whilst the investigation is it ongoing, the actions undertaken so far confirm the extensive use of financial intelligence to develop evidence in this particular case.

Case 2: The FIU submitted to the OPP analysis of several suspicious activity reports. Consequently, documents of a Liechtenstein bank seized by the investigating judge were sent to the National Police with the request for analysis. It was suspected that a Swiss citizen, as an employee of Swiss company sold goods to Russia. The Swiss citizen and his Russian partner and another person from Switzerland received commissions from those transactions. However, there was suspicion that some parts of these commissions were coverage for bribes that had been paid through these transactions. The information provided by the FIU was analysed by the National Police and the suspicion was later confirmed. It formed basis for the National Police, the OPP and the investigating judge to pursue further investigative actions, i.e., examine relevant accounts and seize documents, thus proving that financial intelligence produced by the FIU was a valuable asset in developing this investigation.

184. Some ML proceedings (especially self-laundering) are also initiated as a result of investigations by the National Police in the context of a parallel financial investigation they initiate on their own (see also IO.7 on details how different authorities may initiate investigations). In the course of these activities, the National Police often come across evidence that might indicate elements of ML. In such situations, the National Police initiate an investigation on ML and report it immediately to the OPP.

185. Authorities do not keep separate statistics on the outcome of investigations initiated by the National Police, however, they advised that almost all convictions in smaller self-laundering cases (in particular with domestic commercial theft, burglary and drug trafficking as predicate offences) resulted from investigations initiated by the National Police.

186. During the onsite, the AT discussed all cases of ML investigations that resulted in ML conviction. Four of these cases were initiated by the FIU disseminations (based on an SAR/STR), whilst the rest originate from the information received in incoming MLA requests and, to a lesser

extent, from individual complaints. Whilst these cases had different trigger points for their investigations, in all of them the FIU's analyses of financial intelligence constituted an inevitable part of the operational activities carried out by the competent authorities. As regards the overall number of investigations resulting in indictments and convictions, whilst this might not appear sufficient, one has to bear in mind certain difficulties in gathering evidence from abroad (see IOs 7 and 2, where these issues have been extensively explained). What the AT has observed onsite is that a proactive approach by Liechtenstein authorities in seeking evidence from abroad is not always followed by prompt responses by their foreign counterparts. Consequently, the fact that numerous investigations were initiated as a result of an appropriate use of financial intelligence but were not always followed by indictments or convictions should not signal that there is any specific problem with the FIU's/other competent authorities' assessment and use of financial intelligence to develop evidence and trace proceeds related to ML or predicate offences. This notwithstanding, the overall AML/CFT repressive apparatus in the country (this including the FIU's operational work) needs to invest further efforts in detecting/investigating more sophisticated ML schemes potentially including complex legal structures established and managed in Liechtenstein. Lack of such cases has been further discussed under IO.7.

TF related financial intelligence

187. As for the use of financial intelligence in TF, as provided under IO.9 there has been one case, where FIU dissemination led to TF investigation. In total there has been 13 information requests to the National Police, which included elements related to TF. These requests together with 7 TF related SARs/STRs received during the period under review, although extensively analysed by the FIU and other competent authorities, did not generate any reasonable grounds that TF activity has occurred.

3.2.2. STRs received and requested by competent authorities

SARs/STRs

188. FIU is the central agency for the receipt and analysis of SARs/STRs and these reports are addressed exclusively to the FIU. SAR/STR reporting is the only reporting system, whereby the SARs/STRs relate to the entire business relationship with a customer and are not about a single transaction. There is no exact timeframe established for SAR/STR submission, but SAR/STR must be submitted immediately, as soon as the suspicion arises. The FIU published a guidance on SARs/STRs reporting obligations, which covers issues related to monitoring of business relationship by persons subject to the DDA, conditions for submitting a report (the lowered threshold), elements of the report etc.

189. Reporting is conducted through the go AML electronic reporting system introduced by the FIU in 2018. It also serves as a safe channel of communication (message board web portal) between the FIU and persons subject to the DDA. Since the system's introduction in 2018, persons subject to the DDA were given a 12-month transition period to get accustomed to the new reporting web portal. A report of suspicion is submitted once receipt has been confirmed by the FIU via goAML, as the FIU does not accept reports of suspicion that are incomplete or not submitted in accordance with the requirements. There is a four-eye principle for confirmation of the SARs/STRs. The report is reviewed both from the technical and from the analytical perspective to ensure the completeness of information submitted.

190. Several initiatives were undertaken by the authorities during the period under review aimed at improvement of understanding and compliance with reporting obligations by persons subject to the DDA, including provision of additional guidance on indicators of ML/TF in the DDO (e.g., see section 3.2.3 below) and enhanced focus of the FMA on the matter (generally because of supervisory changes from 2019 onwards and specifically through thematic inspections of banks in 2021). While these efforts are acknowledged, some concerns remain both on the quantity and the quality of reporting by most of the sectors. These are discussed in the paragraphs below.

191. Table below shows the concentration of SAR/STR reporting by different types of persons subject to the DDA:

Table 3.3: SARs/STRs per sector

Sectors	2015	2016	2017	2018	2019	2020
Banks	238	213	152	295	515	844
Public Authorities	10	13	12	7	13	13
DPMS	0	0	0	0	0	0
Dealers in high-value goods	0	0	0	0	1	0
Lawyers	7	7	1	0	0	2
TCSP's	65	54	45	82	131	102
Asset managers	3	0	2	1	1	2
Insurance Companies	28	18	23	30	22	15
E-Money-Institutions	0	0	0	2	1	29
Insurance Brokers	1	0	2	2	0	0
Investment Firms	0	0	0	0	2	0
Auditors	3	0	0	1	5	2
PSP (Payment service providers)	12	10	5	3	5	1
Finance Companies	0	3	2	0	0	0
Life insurers				6	5	4
VASPs						640
Casinos					9	4
Total	**375**	**329**	**259**	**441**	**736**	**1658**

192. With regard to the number of SARs/STRs submitted, there has been an increase in the numbers starting from 2018, especially in the banking and TSCPs sectors. Excluding the effect of entry of VASPs into the market, the significant increase in reporting is, in large part, due to: (i) supervisory changes from 2019 onwards; (ii) enhanced FIU communication (through guidance

and outreach) that the SAR/STR obligation does not require the identification of a predicate offence; and (iii) message sent to the private sector through a number of prosecutions for failing to make reports in line with the DDA, and two subsequent convictions, the first of which was in 2018 (see IO.7).

193. On average, 70% of SARs/STRs come from the banking sector, which is commensurate with its share of the total assets and diversity of products/services offered. Nonetheless, certain persons subject to the DDA, such as TCSPs, given the risk profile of their activities as observed in the NRA II, are expected to have a more significant contribution in terms of SAR/STR reporting compared to the current practices (see further IO.4).

194. As regards the quality of the reports submitted to the FIU, one of the parameters for assessing the appropriateness of the reporting obligation would be consistency of the SARs/STRs with the main threats prevalent in the country. Statistics provided in Table 3.4 are mostly consistent with the risk of predicate offences discussed under NRA-ML. The only exception concerns lack of tax offences related SARs/STRs.

Table 3.4: SARs/STRs - Statistics on predicate offences

		NRA ML threats classification	
2016-2018	**SARs /STRs**	**Predicate offences abroad**	**Predicate offences domestically**
Fraud, criminal breach of trust and embezzlement	570	High	Medium-High
Corruption and active bribery	110	High	Low
Theft and robbery	-	Medium-Low	Medium
Tax offences	26	Medium-High	Low
Insider dealing	-	Medium Low	Low
Narcotic offences	19	Medium	Medium-Low

Another important development concerns amendments to Art. 165(5) of the CC which now criminalises any execution of a banking transaction in relation to illegitimate tax savings (transfer of such asset components to a third party) and banks, their employees and management bodies could be held liable for ML if they transfer such asset components to a third party. This reform has resulted in termination of a large volume of business relationships. Authorities advised that 41 SARs/STRs in 2019 and 77 in 2020 filed by the banks could be linked with this reform. Whilst IO.4 discusses the SAR/STR reporting on this particular matter in more details, majority of these SARs/STRs resulted in FIU spontaneous dissemination to their foreign counterparts in a form of the statement of fact, and, where relevant, were also sent to the Fiscal Authority. The AT was informed that, so far, no further developments were observed regarding these disseminations.

195. The FIU considers the content and description of the SARs/STRs to be generally adequate, although they do not always include all information needed for subsequent analysis. This issue has been remedied by an introduction of an FIU power to request information from persons

subject to the DDA regardless of the circumstances of the case and whether or not prior SAR/STR was submitted.

196. Persons subject to the DDA are obliged to answer to the FIU request for additional information in 3-5 working days. The FIU advised, that persons subject to the DDA (with one exception) provided information promptly. In this exceptional case, the reason behind this lack of response by a reporting entity was technical (they did not check the goAML inbox). As a result, the reporting entity was sentenced to a fine by the court.

Table 3.5: FIU additional requests sent to persons subject to the DDA*

Sectors	Banks	TCSPs	VASPs	Insurance companies	Life insurance companies	Auditors	Asset managers	Investment funds
2018	245	60	N/A	7	1	0	1	0
2019	280	61	N/A	8	1	0	0	2
2020	221	54	26	9	0	1	0	2

**The statistics provided do not include data for the years before 2018, as within the previous case management system used before the goAML, the requests sent to persons subject to the DDA were not counted as additional request but were considered as new ones.*

197. As regards the use of SARs/STRs by the competent authorities, the analysis of the latter highlights a downward trend in 2019 and 2020 despite the increase in the number of reports filed (statistics for 2021 was not available). Discrepancy in the numbers for the year 2020 is a result of the introduction of a large VASP, which submitted significant number of SARs/STRs. In that regard, this discrepancy does not signal that there is any significant decrease in quality of SARs/STRs received. On the other hand, the statistics provided above does not support the authorities' views that quality of SARs/STRs has significantly improved – in terms of their usage for disseminations to LEAs the figures remain stable throughout the period under review (2015-2020).

Table 3.6: Statistics on the use of SARs/STRs in disseminations

Year	2015	2016	2017	2018	2019	2020
Total no. of SARs/STRs	375	329	259	441	736	1671
Total number of SARs/STRs used in reports sent to OPP	191	170	94	326	265	204
Total no. of cases forwarded to LEAs	191	170	93	138	131	115
Ratio SARs/STRs filed/ SARs/STRs used in reports	**51%**	**51.6%**	**36%**	**74%**	**36%**	**12%**

198. As per the complexity of cases identified based on the SARs/STRs, the analysis shows that the SARs/STRs mostly relate to self-laundering. SARs/STRs which concern more complex cases

are usually filed reactively, only after receipt of an inquiry from authorities. This is also confirmed by the findings of the NRA ML, where the authorities observe a constant tendency towards late reporting. This means that suspicious activity/transaction report is submitted by a person subject to the DDA as a result of hits in commercial databases or publicly available sources only after specific information has been requested by competent authorities. To that end, the AT has some concerns on the extent to which persons subject to the DDA identify suspicious transactions/activities that might be part of more complex ML schemes.

199. Starting from year 2015 to 2019, the FIU received 7 SARs/STRs related to TF, from which one was disseminated to the OPP. Other SARs/STRs had very few links to TF and no suspicion was confirmed (see IO.9). Financial flows from and to high-risk jurisdictions constitutes 0.9% of the total volume of funds. Whilst this percentage does not appear significant, the overall amount of these transactions is considerable (around CHF 2.7 billion – see IO.1 and IO.9). Consequently, the fact that only seven SARs/STRs were submitted by persons subject to the DDA might indicate that persons subject to the DDA were not always vigilant enough in exercising their duties in relation to suspicious transactions related to TF. The issue on SAR/STR reporting regime, in particular the systemic reactive and late filing was also noted under NRA-TF II, "calling into question the effectiveness of the national compliance framework, and, as a consequence, the ability of the private sector to properly identify and report TF-related suspicion". At the same time, when onsite, the AT observed that persons subject to the DDA have appropriate level of awareness on TF related reporting (see IO.4), and the FIU efforts in this direction also appear adequate. This notwithstanding, the competent authorities, primarily the FIU and supervisors, need to continue working on this matter and ensure that the risks brought by a high volume of transactions with high-risk jurisdiction are properly reflected through the SAR/STR reporting too.

Feedback

200. The FIU provides feedback to persons subject to the DDA in individual cases either through phone calls or through scheduled in-person discussions at the FIU's premises, especially when persons subject to the DDA seem unsure on whether or not a certain client relationship is to be reported. Authorities consider these meetings as a knowledge transfer tool and lead to persons subject to the DDAs' improved understanding of how the reporting requirement is to be interpreted.

201. The FIU gives annual feedback to those persons subject to the DDA that file a significant amount of SARs/STRs, and these are considered as "management discussions". While only part of persons subject to the DDA met on-site confirmed receiving feedback from the FIU on the cases submitted, they were very satisfied with the establishment of the Public Private Partnership (established by the FIU with the banking association and their member banks in 2020), a platform for regular discussions on various issues with the authorities. Prior to the introduction of this platform, the FIU used to get back to the person subject to the DDA individually or at a group level on topics such as typologies and associated findings. Public private partnership meetings have, so far, had the following items on its meetings' agenda: (i)Sanction evasion typologies, (ii) crypto risk exposure for private banks, (iii) risks related to VASPs in Liechtenstein (general trends, methods and other observations), (iv) art industry ML threats, (v) discussion of international PPP models, (vi) general TF typologies.

Cross-border cash information

202. Liechtenstein adopted a disclosure system for cross-border transportation of currency and bearer negotiable instruments (BNIs). The Swiss Border Guard Corps carries out cash controls at the Liechtenstein border crossing posts to Austria. In case of truthful disclosure, the disclosure form is transmitted to National Police, however, there has been little evidence on use of this information for purposes of ML/TF investigations (see IO.8).

203. The FIU does not have direct access to the Swiss Customs' databases which contains the information about declarations of cross-border currency transportation and ancillary offences. This information would reach the FIU through the National Police - once they receive it from Swiss Customs they would transmit it immediately to the FIU. The latter receives both, the entire list of cash disclosures (every three months) made at the Liechtenstein-Austrian border from persons entering Liechtenstein as well as SARs/STRs concerning cash-disclosures, which are filed by the National Police as soon as the suspicion arises.

204. The National Police has the legal obligation to also report such cases to the OPP without delay. In practice, the National Police has filed 14 SARs/STRs on cross-border cash transportation for the period 2016-2021 upon receiving such information from Swiss Customs. In most of the cases the FIU analysis did not reveal any connection to Liechtenstein, while 2 cases were further analysed (see IO.8), where cash was seized at the border and when the OPP initiated a ML investigation. The analysis could not substantiate initial ML suspicion.

205. The National Police can provide the FIU with certain details of equivalent controls made by their Austrian counterparts once travellers have left Liechtenstein and passed Swiss Customs. This was applied in one case in 2020, where the FIU learned from different newspaper articles that a group of foreign nationals were caught with a substantial amount of gold by Austrian Customs at a non-strictly controlled border crossing point in the very north of Liechtenstein. The FIU used this information to request additional information from affected persons subject to the DDA in Liechtenstein. However, no information was provided on the outcome of the case to confirm the use of cross-border information to investigate ML.

206. Overall, the AT is of the view that the system in place merits further improvements to enable better cross-border cash transportation control as further elaborated under core issue 8.3.

3.2.3. Operational needs supported by FIU analysis and dissemination

FIU's structure and resources

207. The FIU is an administrative office within the Ministry of General Government Affairs and Finance. The FIU has two departments, operational and strategic analysis. It has 12 employees, including the head of the FIU. Operational analysis department is composed of the head of department and five analysts, two of which are part time. Strategic analysis department includes the head of the department and senior strategic analysis officer and two IT specialists. All staff members have access to goAML and other mining tools, as the strategic analysis department is often involved in the process of operational analysis, taking into account the latter's workload.

208. The FIU staff members together with other competent authorities are regularly trained. The FIU has the necessary infrastructure, including physical and IT security measures, for safe receipt and storage of all reports and other disclosures.

209. Though the FIU is composed of skilled and motivated professionals, the steady increase of SARs/STRs received, in conjunction with new challenges (VASPs' SARs/STRs and related typologies) and some recent high-profile cases, which are still at their initial stage, require serious considerations on whether the current human resources are sufficient to adequately deal with such a heavy workload.

210. The administrative procedure for hiring new staff in the FIU starts with the proposals to the competent Ministry for General Government Affairs and Finance. If accepted, the decision is then subject to parliamentary approval during regular parliamentary sessions at the end of a year[13].

Operational analysis

211. The following sources of information form basis for the FIU to start operational analysis: (a) SARs/STRs received from persons subject to the DDA; (b) information transmitted from the OPP, source of which are incoming MLA requests/spontaneous information received by police; (c) open-source information and (d) disseminations/requests received from foreign FIUs.

212. When the SARs/STRs are received, the system alerts if there is a link with the existing case and if there is a match with the existing case, the SAR/STR is escalated to the case. If there is high probability of match with the existing case, verifications are made on whether the subjects are connected.

213. The FIU prioritises cases (SARs/STRs) against a certain set of criteria (internal database hits, links with ongoing criminal investigations/ proceedings, international context (incoming MLA), involvement of PEPs, volume of assets involved, TF, etc.) and as a result, a risk score is assigned. For SARs/STRs received from VASPs, some other criteria (exposure to darknet, addresses linked to illegal VASP activity, identity theft etc.) are used for prioritisation purposes. The Head of the Operational Analysis Department assigns cases according to the current capacities and expertise of individual analysts. TF cases and requests from foreign FIUs are set with the highest score.

214. Where a lower risk score is determined, the case is assigned to a pool of case proposals for later consideration. Less than 5% of cases (SARs/STRs) are not analysed, most of which concern the cases where the SAR/STR is received without existing business relationship or there is only a need to spontaneously disclose information to a foreign FIU. Prioritisation is always conducted with the combination of risk score and materiality. The FIU advised that before the introduction of goAML in 2018, the FIU counted cases differently. From 2002 until 2018 each SAR/STR, each domestic request as well as each foreign request (MLA/FIU-request) automatically created a case within the previous database infrastructure. With goAML, cases can entail multiple SARs/STRs, additional requests for information as well as responses by persons subject to the DDA, associated foreign requests etc.

215. The FIU has several IT tools that allow for data mining and further analysis, such as goAML (central case database, entailing basic analytical tools for mining), i2 iBase and InfoZoom. goAML also serves as a secure communication channel between the FIU and persons subject to the DDA/ authorities. Before, the FIU received all communication with persons subject to the DDA and/or

[13] After the on-site, based on the 2022 budget 2 new positions were opened for the FIU.

authorities in paper form. The data was then imported to the FIU database for further analysis. At the moment, the data contained in the old system has not yet been transferred to the goAML, thus both databases are used in the course of FIU analysis. While the searches in the goAML are automated, the ones done in the previous database are manual. For the purpose of analysis of SARs/STRs received from VASPs, Chain Analysis Reactor is being used. Data and information kept with the FIU are protected and run on separate servers with the Office of Information Technology.

216. The FIU Analysis Manual provides for the analytical process starting from analysis techniques, types of operational analysis, prioritisation and pooling process, types of strategic analysis etc. It is a confidential document, content of which was presented to the AT. There is no exact timeframe on the duration of the analysis. From what the AT could observe during the interviews held onsite the Manual presents a solid basis for FIU staff operational analysis. Whenever a case is created from an intelligence perspective, then the analysis must be carried out. A case can be multi-faceted and include (i) one or more SARs/STRs from one or more persons subject to the DDA, (ii) MLA request(s), (iii) replies by persons subject to the DDA to the FIU and LEAs on cases already open by their side.

217. During the years 2018- June 2021, 673 analytical products were disseminated by the FIU, of which 569 were sent to the OPP, 2 to the Court of Justice on newly emerged facts and 83 to the FMA. The latter concerns reports on specific persons subject to the DDA aimed at supporting FMA's supervision over their AML/CFT compliance. Between 2018 and 2021 (October) 72 requests have been made to the FIU for additional information. Some other authorities also receive FIU's analytical products, but these are limited to cases which directly concern their areas of activities (e.g., STIFA issues concerning NPOs; Fiscal Authority- issues concerning tax, etc.). The analysis of simple cases lasts couple of days, whereas complex cases can last for weeks.

218. As for the reporting year of 2020 onwards, in a significant number of crypto-related SARs/STRs no referral to the OPP was made due to the lack of jurisdiction over those cases (i.e., unauthorized access, stolen funds cases etc.). In those cases, the FIU sends information to affected foreign counterparts. This explains (i) the downward trend of the total no. of SARs/STRs received vs. total no. of SARs/STRs being used in analytical reports sent to LEAs and (ii) the large number of spontaneous disseminations sent to foreign counterparts (see also IO.2).

Table 3.7: Statistics on cases analyzed

Year	2015	2016	2017	2018	2019	2020
Total no. of cases analyzed[14]	368	318	257	448	329	1474
Total no. of cases pending[15]	7	11	2	13	6	
Total no. of cases forwarded to LEAs	191	170	93	138	131	115
Investigations launched		55	93	44	43	50
Ratio Dissemination/investigation		**32%**	**48%**	**32%**	**33%**	**43%**

219. The statistics above show that 170 disseminations resulted in 55 investigations in 2016 (32%), 93 disseminations in 45 investigations in 2017 (48%), 138 disseminations in 44 cases in

[14] In a given year.

[15] At the end of the year.

2018 (32%), 131 disseminations in 43 cases in 2019 (33%), and 115 disseminations in 50 investigations in 2020 (43%).

220. Another source of information used by the FIU is the information or requests received from their foreign counterparts and operational analysis based on the screening of media reports.

Box 2

FIU dissemination to the OPP based on other information resulting in investigation

The FIU came across the following information when conducting thorough OSINT research in relation to a large-scale case involving a South American jurisdiction. The information contained in this article indicated that a former foreign minister of a South American jurisdiction had purchased gold in Liechtenstein using funds held with their offshore company account in Liechtenstein. This triggered an analysis conducted by the FIU into all domestic entities affected by this business deal (the bank, the precious metals dealer as well as local TCSPs). The analysis revealed that the gold had been picked up by a third party that was already known to have ties with a large-scale ongoing international investigation. Analytical report was then prepared and sent to the OPP. The National Police, upon OPP's request, interrogated the TCSP concerned, as well as the precious metals dealer (not subject to due diligence) thus acquiring additional information and evidence needed to pursue investigation, which is still ongoing.

Strategic analysis

221. The FIU has so far produced several comprehensive strategic analysis reports. They are based on trends and methods explored by the Egmont Group.

222. The strategic analyses conducted by the FIU can be combined in 3 groups: (a) Situational reports that are prepared on the specific countries' risks, including typologies observed in these countries. These reports are not published; (b) Typologies, risks, methods, and trends identified through the FIU's operational analysis. These are shared with persons subject to the DDA through the FIU's annual report and the Public-Private-Partnership platform; (c) Restricted reports on typologies, risks, methods, and trends which are only shared with the government, the FMA and in some instances other affected authorities to nurture decision-making processes (including NRA processes). Another example of strategic analysis are the status reports, such as the one on VASPs that the FIU initiated in December 2020, the results of which were disseminated to the FMA. At that time only one on-site visit on VASPs was conducted by the FMA, thus the report assisted the FMA in providing a broader picture of the sector and its specific risks (including the use of falsified IDs).

223. The activities carried out with regard to strategic analysis are to be commended. These analyses are of a good quality, and they serve it purpose given the risks and context of the jurisdiction. In addition, the AT finds important to mention several other actions. More specifically, further to the amendments to the Art. 165(5) of the CC which resulted in termination of substantial amount of business relations, in May 2019 trainings were held for the persons subject to the DDA on their obligations in this regard. Public-private partnership platform was used for this purpose. Furthermore, Section V was added to the Annex 3 of the DDO, documenting the interpretation of the authorities and providing guidance to persons subject to the DDA regarding tax offences. This notwithstanding, this area needs to remain in the FIU's focus, including its further analysis on appropriateness of SAR/STR reporting on this matter.

224. As regards strategic analysis on TF, some typologies (TF related crypto case and using of NPOs for TF purposes) were published in 2021 casebook. Whilst these analyses are useful for persons subject to the DDA, issues previously discussed on SAR/STR reporting in relation to inflows and outflows from/to TF related high risk jurisdictions warrant further analysis. Although it is a subject to PROTEGE WG discussions, the authorities acknowledged the need to continue with their efforts in this area.

225. In addition, the AT believes that the authorities would further benefit from developing TF-related typologies based on the risks identified under the NRA-TF, which would also cover the use of cash.

Suspension of suspicious transactions

226. The DDA empowers the FIU to suspend transactions (including assets) which might be connected with ML, predicate, organised crime or TF for a maximum period of two working days. This tool enables immediate reaction and freezing of funds before a court order is obtained, thus preventing dissipation of assets. Table below shows that this power has been extensively used to seize/secure funds which are suspected to derive from criminal activities.

Table 3.8: Assets frozen based on FIU information

	Assets frozen based on FIU reports		**Total assets frozen**		*Ratio %* *Amounts based on FIU report/ total*
Year	Cases	Amount (EUR)	Cases	Amount (EUR)	
2015	23	117 228 673	28	121 658 174	*96%*
2016	21	62 177 783	22	62 181 874	*99%*
2017	11	112 243 889	16	115 874 722	*97%*
2018	29	491 433 241	36	499 425 958	*98%*
2019	16	517 572 239	20	518 308 490	*99%*
2020	18	86 586 425	24	87 980 475	*98%*

3.2.4. Cooperation and exchange of information/financial intelligence

227. Interviews and statistical data on the number of information requests sent by LEAs to the FIU, together with the case examples presented, confirm that there is extensive cooperation and information exchange on a regular basis. The size of the jurisdiction allows prompt information exchange and consultations among all the relevant authorities.

228. The FIU advised that in general, they receive the information requested from public authorities, although in individual cases additional requests are sent in order to get the full information, which occurs due to certain misunderstandings of content requested or of technical formulations used in the request.

229. The FIU has indirect access to certain types of administrative, financial and law enforcement information (see table above) and to receive it, it needs to address a formal written request. Authorities advised, that from time to time a certain time delay is caused in receiving responses, so the FIU considers having direct access to this information would be of benefit.

Table 3.9: FIU requests sent to domestic authorities

Authorities	2015	2016	2017	2018	2019	2020
OPP	1	9	9	31	57	46
National Police	70	62	31	48	69	48
Fiscal Authority	1	1	0	1	3	2
FMA	2	3	2	1	6	6

230. As already noted, the FIU uses goAML channel for information exchange with persons subject to the DDA, the FMA, the STIFA and the Fiscal Authority. The disseminations to the OPP are sent with internal postal service and paper copies are directly delivered to the prosecutor designated to the case.

231. The OPP, the National Police and investigative judges obtain information, especially BO and other CDD information, from the FIU in ongoing investigations of ML, associated predicate offences and TF, in non-conviction-based proceedings for tracing of criminal proceeds, as well as when an MLA is received from foreign jurisdictions. A declaration of cooperation was signed between the Court of Justice, the OPP, the National Police, the FMA and the FIU in March/April 2020, which regulates the cooperation in criminal and judicial proceedings. During the years from 2018-2020, 262 requests of information/analysis were sent to FIU, of which 126 from the National Police, 18 from the OPP, 70 from the FMA and the remaining 48 from other authorities All of the requests were duly answered, and the recipient authorities were satisfied with the quality of these responses.

232. Before April 2021, obtaining information from the Fiscal Authority was subject to specific procedures, which were also time-consuming. Starting from April 2021, this obstacle has been removed by introduction of provisions in the DDA which includes Fiscal Authority among those required to work together in close cooperation to provide each other with all information that is necessary for enforcement of the relevant AML/CFT legislation.

233. Cooperation between the FIU and other competent authorities is also ensured through the PROTEGE WG. The terms of reference and discussions held within this working group are discussed under IO.1. In addition, a bimonthly exchange between representatives of FIU, the OPP, FMA, STIFA and the Fiscal Authority takes place to discuss potential cases, supervisory cases, as well as measures/sanctions. These meetings are coordinated by the FMA.

234. Overall, there is an extensive cooperation and information exchange on a regular basis among competent authorities. This presents a strong component in the overall AML/CFT system in the country.

Overall conclusions on IO.6

235. Liechtenstein FIU constitutes an important source of financial intelligence information which facilitates investigations of ML, TF and predicate offences in Liechtenstein. It has access to a wide range of financial, administrative and law enforcement information and this power has been extensively used to analyse data and information received from persons subject to the DDA, foreign counterparts, and competent authorities. Law enforcement and other competent authorities largely benefit from financial intelligence produced by the FIU in the course of their financial investigations.

236. Whilst both operational and strategic analysis present a strong feature of the overall AML/CFT system in the country, some areas still warrant more attention and strategic approach.

237. The quality of the SARs/STRs received by the FIU is considered appropriate although they are yet to be fully aligned with some of the threats identified (i.e., tax offences committed abroad).

238. The members of the FIU are well experienced and are able to produce high quality intelligence. Cooperation and exchange of information between the authorities represents one of the strengths of the system.

Liechtenstein is rated as having a substantial level of effectiveness for IO.6.

3.3. Immediate Outcome 7 (ML investigation and prosecution)

3.3.1. ML identification and investigation

239. Liechtenstein has criminalised all forms of ML as required by R.3. This bears particular relevance for an IFC and provides necessary basis to deal with ML threats stemming from predicate offences committed abroad. The institutional framework is also in place, where the OPP is ex officio in charge to investigate all criminal offences, including ML and its predicates. For this purpose, the OPP may request the National Police or the investigating judge to carry out investigations. In case the OPP hands over the investigation to one of these institutions, the office would then not have a direct involvement in execution of the investigatory actions (e.g., interrogate suspects and witnesses, take part in house searches, etc.) but would receive all evidence gathered, and then either drop charges or indict those concerned. The National Police may also, on their own, initiate investigation once they come across any evidence/indices that a crime was committed. De jure, they are obliged to investigate every criminal offence which has been brought to their attention and has to, without delay, carry out inquiries. Once they initiate investigation, they inform the OPP and the investigative judge. The National Police consults the two institutions on steps to be undertaken in the course of their investigation. As, discussed above, once the relevant materials/evidence are gathered they are then handed over to the OPP and/or investigative judge. In general, majority of ML related investigations are carried out by the OPP where National Police provides executive assistance.

240. There are 8 prosecutors in the OPP and 4 investigative judges who are in charge for investigations in Liechtenstein. The OPP has designated two public prosecutors who are specialised in the investigation and the prosecution of ML and associated predicate offences. In the Economic Crime Unit at the National Police two financial investigators are specialised in ML investigations and associated predicate offences. Level of domestic criminality is very low thus allowing their focus to be placed on ML activities in the country stemming from criminal offences

committed abroad. As a consequence, the OPP and the National Police regularly investigate financial elements of predicate offences and develop parallel financial investigations which aim is twofold: (i) to identify proceeds of crime, and (ii) to identify the way these proceeds were laundered or attempted to be laundered through Liechtenstein FIs, DNFBPs or VASPs. Interviews held on-site confirmed that prosecutors, investigative judges, and police officers possess relevant skills and knowledge on how to pursue ML. They are very motivated and focused on developing their expertise in this area which is considered to be a priority. They take part in specialised trainings regularly.

241. The relevant case law, including the decisions of the Constitutional and Supreme courts which derive from the jurisprudence established in Austria, suggest that the level of proof required for initiating a ML investigation is relatively low, especially concerning the extent to which the predicate offence needs to be established. The afore-mentioned decisions state that ML suspicions '*cannot be dissociated from the suspicion of a predicate offence, and, in view of an initial suspicion of ML, there is no need for indicators of a concrete predicate offence*'. These developments set an appropriate basis for initiating ML investigation when predicates are committed abroad and when only indices rather than direct evidence on these predicates are available. This is an important tool in Liechtenstein's AML regime that helps financial and ML related investigations/prosecutions to proceed without the need to prove the specific predicate. As a consequence, the authorities classify 65% of investigations as autonomous/stand-alone ML cases. This figure, however, includes all ML related investigations where predicates were committed abroad, regardless of whether a conviction on predicate offence was achieved or not. In other words, all ML related investigations which, as their starting point, have a conviction for a predicate offence achieved in a foreign jurisdiction, if prosecuted, are classified as stand-alone/autonomous ML. Consequently, the statistics in relation to stand-alone/autonomous ML is substantial, where majority of these investigations derive from convictions on predicate offences obtained abroad. Whilst not disputing the authorities approach to make such classifications the way they deem appropriate, the AT notes that it is not fully in line with the relevant footnote attached to Core Issue 7.3 of the FATF Methodology which defines stand-alone (autonomous) ML as a process where the prosecution of ML was done independently from the predicate, with emphasis that it is relevant in cases where there is insufficient evidence of particular predicate offence or where there is a lack of territorial jurisdiction over the predicate offence. Since July 2019, Liechtenstein judicial system also permits trials in absentia (Art. 295 of the CPC) – as long as the suspect has legal representation. That legal representation is achieved, if necessary, by appointment from the court. This feature facilitates the trial (and likely conviction) of defendants who are not present in Liechtenstein. On the other hand, this provision is an incentive for foreign suspects to personally appear in a trial before the Liechtenstein courts.

242. Whilst this vigorous approach to opening financial/ML investigations is to be commended, the assessment team also observed that a large number of these investigations remains open for a considerable period of time. Table 3.10 below shows that, so far, less than 10% of investigations resulted in indictments. The reasons that so many ML investigations do not lead to a ML prosecution may be manifold. It may include lack of resources, insufficient expertise in financial matters, high threshold of evidence required for obtaining conviction, lack of cooperation by foreign counterparts, etc. The authorities were firm that this percentage results exclusively from the problems they encounter when seeking assistance from foreign jurisdiction - the lack (or very slow provision) of cooperation by the countries where predicates were

committed or where suspects reside, is the key and probably the only obstacle they have. In addition, they emphasised that it takes time to collate and verify such evidence, as many times information received is incomplete or inaccurate. The AT, to the extent to which it had an insight into ML cases presented during the on-site, agrees, to a large extent, with the reasoning put forward by the authorities. Given the cases presented and discussed, it became apparent that ineffective cooperation by some jurisdictions had a significant impact on further developments in already initiated ML investigations.

Table 3.10: ML investigations, indictment, convictions and acquittals

	Investigations for ML			**Indictments** for ML			**Convictions** for ML			**Acquittals**
Year	Cases	Self-ML	Autonom[16]. ML	Cases	Self-ML	Autonom. ML	Cases	Self-ML	Autonom. ML	
2016	89	34	55	7	3	4	5	4	1	1
2017	86	39	47	20	16	4	8	6	2	0
2018	77	33	44	12	8	4	8	7	1	1
2019	91	41	50	20	15	5	14	10	4	0
2020	121	60	61	12	8	4	13	10	3	2

243. Fraud is the most heavily investigated predicate for ML. In many cases, in addition to fraud, criminal breach of trust or embezzlement, as concurrence offences, are also committed. These predicates are directly or indirectly related and that is the reason why they were put together by the authorities for analysis of ML investigations stemming from them. Fraud (and consequently criminal breach of trust and embezzlement) accounts roughly for 70% of all ML investigations during the period under review. The 2020 NRA states that from 2016 to 2018 fraud, criminal breach of trust and embezzlement committed abroad were predicate offences in 137 ML investigations resulting in almost EUR 590 million being frozen in the course of these proceedings. 12 indictments were raised, and 2 convictions have been handed down. A total of EUR 365 000 was declared forfeit. This NRA finding was also a subject of on-site discussions, and the AT, in support to this finding, also observed that the substance of MLA requests received during the 2016-2018 period largely mirrors what has been said in the NRA – vast majority of

[16] The term 'autonomous ML' in all three columns of this table was used by the Liechtenstein authorities for all cases where predicate offence was committed abroad regardless of whether the ML prosecution in Liechtenstein was initiated after the trial for the predicate commenced or was completed in these other jurisdiction. The AT discussed this issue in the previous paragraphs, and it concluded that this classification as made by the Liechtenstein authorities is not in line with the FATF Methodology. However, the AT kept this table in the report to reflect the statistics as provided by the authorities.

MLA requests (both incoming and outgoing) were in relation to fraud, criminal breach of trust and embezzlement. This is even more evident when analysing the outgoing requests only.

244. ML related to foreign predicates other than fraud (corruption, drug trafficking, tax crimes, etc.) tends to be more challenging to investigate. Indications that the proceeds of these predicates were laundered or that the layering stage of the ML process (i.e., funds shuttle through Liechtenstein FIs, DNFBPs or VASPs to other jurisdictions), are often not a part of the MLAs received. Consequently, the FIU's/persons subject to the DDA' role appears essential - in detecting this type of criminality (through SARs/STRs/analyses/outgoing requests/spontaneous disseminations). SARs/STRs indicating suspicions of ML stemming from predicates other than fraud rarely advance to further stages (i.e. investigations). Authorities advised that the sole reason behind this is a lack of cooperation or insufficient information received by foreign counterparts upon receiving the FIU's requests for information which are made during the course of their analytical process. As it was noted above, the AT could not identify any other reasons for not advancing with these cases but given the risks and context of the jurisdiction it is certain that more efforts need to be invested in this area. This is also acknowledged in the 2020 NRA.

245. Turning to the investigative and prosecutorial process, essentially there are three different triggers for ML proceedings in Liechtenstein (see also IO.6). A large part of ML proceedings is initiated on the basis of MLA requests received from foreign jurisdictions, which are often accompanied by the FIU reports. As a matter of fact, these FIU reports are produced right after an MLA is received and they include analysis/information on money pathways and transactions made by those individuals/entities identified in the request. Other than this, ML investigations are also triggered solely by the FIU reports, whist a number of self-laundering cases resulted from findings of the National Police in the course of their financial investigations.

246. Roughly 50% of investigations were initiated independently from the FIU. These investigations were triggered by intelligence/evidence gathered by (i) police (information gathered in the course of their investigative actions, information received from foreign counterparts, informants, or media) or the OPP (based on information received in the incoming MLA requests).

247. There seems to be no impediment to inter-agency cooperation and coordination with regard to ML investigations/prosecutions, including the timely access to relevant financial intelligence, BO and other information that is needed to build a case. Joint investigations and information exchange between different authorities are possible and occur in almost all ML cases.

248. As already noted, ML investigations, in majority of cases, are initiated upon investigations of a predicate offence in a foreign country, results of which are sent to Liechtenstein (mostly in a form of an MLA but sometimes also through informal cooperation channels). Once an MLA request is received, the competent authorities, primarily the OPP and investigative judges, would engage the National Police and the FIU to further examine potential laundering activity in Liechtenstein. The FIU would, as a matter of urgency, carry out financial intelligence analysis, would further liaise with FIs/DNFBPs/VASPs in case they need additional information and then would duly provide the investigators with elements needed to open a ML investigation. The OPP may also initiate a creation of an inter-institutional sub-group which would deal with a specific case. Such sub-groups are built in complex ML/predicate offences cases, and are composed of the representatives from the OPP, FIU, National Police, and the FMA. Depending on the nature and complexity of the case, investigating judge and tax authorities may attend the sub-group

meetings. The authorities advised that this form of operational cooperation allows them to properly coordinate the procedural measures when deciding to launch an investigation. The sub-groups meetings put forward a clear investigative strategy which discusses next steps and concrete actions by all interlocutors.

249. Specific attention is being placed on avoiding potential tipping off in cross border ML cases due to the rights of the entitled parties in the MLA proceedings to be heard by the court in Liechtenstein prior the incoming MLA request is executed. This issue is discussed in detail under IO2 and it is mentioned here as it may bear relevance in cross-border ML cases.

250. For purposes of ML/predicate offences investigation, the competent authorities apply different investigative means which are at their disposal (see also R.31). To the extent that the AT had an insight into ML cases investigated so far, these investigative means appear to be frequently applied. To confirm this statement, the authorities also presented to the AT a complex case, where investigation is still on-going and where the authorities managed to seize computers and communication devices which were a source of important evidence. Given the high profile of this investigations, its cross-border elements and involvement of number of persons and jurisdictions, further details could not be elaborated for confidentiality reasons.

251. Forensic accounting may be made available to the investigative authorities upon their request. This possibility does not seem to be often materialised since the authorities believe that they are well equipped with knowledge in this area, with the FIU specialists being available for reconstruction of transactions and any other expertise in the financial crime area.

252. Up until 2017, ML proceedings were carried out almost exclusively against natural persons for self-laundering and mostly against the offender of the predicate offence, against account holders or against BOs of entities which were holders of the accounts where illicitly gained funds were placed. Since 2018 competent authorities have initiated several ML investigations against legal entities, some of which are FIs and DNFBPs. The 2020 NRA acknowledged that since 2017 the OPP refocused on ML inquiries against persons subject to the DDA. This notwithstanding, the cases where convictions against legal persons were achieved are yet very simple and straight forward ML cases, example of which is elaborated in the box below. On the other hand, some recent investigations which involve legal entities established in Liechtenstein include more sophisticated ML schemes. In one case, a Liechtenstein corporation was allegedly involved in tax fraud and ML stemming from activities in several jurisdictions. The approximate loss in taxes in a neighbouring jurisdiction was estimated at EUR 23 million. Another high-profile investigation addresses a chain of fraudulent activities carried out in several jurisdictions. This cross-border investigation includes a financial service provider based in Switzerland and in Liechtenstein – one of the suspects acted as an intermediary for a South American state companies. On the basis of money flows analyses, a large global structure orchestrated the transactions, and the Liechtenstein bank was about to be used as a transaction processing centre. Further details of these investigations are confidential. AT is clear that these are serious and thorough on-going investigations. It remains to be seen how they develop and what their final results will be.

Box 3 - ML investigation involving a legal person

Based on a complaint filed by injured party, the OPP opened an investigation for suspicion of fraudulent bankruptcy and self-laundering. Two offices were searched. Documents and other evidence were then seized. In addition, a Liechtenstein bank was ordered to surrender account and banking information. The National Police carried out financial investigations and analysed a large amount of evidence, questioned a number of witnesses and suspects. In August 2018 the OPP indicted the defendant and his wife charging him for fraudulent bankruptcy by transferring real estate to his wife, who contributed the properties to a family foundation, and for transferring around EUR 357 000 form his accounts to various accounts of the family foundation. The defendant also was charged for self-laundering as he acted as board of trustees of the family foundation. The foundation also was charged for ML. The defendant was convicted in November 2018 for fraudulent bankruptcy and self-laundering. His wife was acquitted. The family foundation was held responsible for ML committed by the defendant (as board of trustees of the family foundation) and was fined with 50 daily rates (one daily rate CHF 200) to a total fine of CHF 10 000. All the assets of the family foundation (real estate and funds on bank accounts) were confiscated.

253. Overall, during the period under review a total of 464 ML investigations were open. These investigations target 874 individuals and 176 legal persons, among which are the banks, TCSPs and insurance companies, as well as the representatives or employees of FIs and DNFBPs.

Table 3.11: ML investigations

Investigations for ML				
Year	Cases total	Persons total	Natural persons	Legal persons
2016	89	215	198	17
2017	86	140	129	11
2018	77	182	147	35
2019	91	210	153	57
2020	121	303	247	56

254. According to the statistics provided by the authorities, so far indictments were rendered in 71 of these cases, whilst 48 convictions and 4 acquittals were achieved. In 2020, the figures confirm the trend of having more investigations against legal entities and against bank employees and trustees. The results of these investigations are expected to be seen in the near future. The AT finds this encouraging and welcomes the authorities' focus on ML cases which might involve activities of third parties.

255. The figures presented above are also very high and trigger resources implications. Although the AT is aware that the vast majority of these cases are simple and straight forward ML investigations, it remains concerned if the competent authorities (OPP, judiciary, the FIU, National Police) are sufficiently resourced to deal with this number of cases. This is even more apparent when considering some recent and very complex ML investigations which are, as mentioned in previous paragraphs of this IO, at early stages. Handling these cases simultaneously with the on-going investigations in a timely manner with current resources seems rather difficult.

The AT is of the opinion that more prosecutorial and investigative resources with significant practical experience in financial crime is needed.

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

256. Investigations and prosecutions of ML in Liechtenstein are, to some extent, in line with the overall risk profile of the country. This conclusion is partly related to the methodology used by the authorities to develop the NRA – as it is observed under IO.1, the NRA took into account the existing typologies/cases/ML activities investigated and prosecuted in recent years. Consequently, the predicates to ML offences that occurred in Liechtenstein were a basis for the threat analysis in the NRA.

257. Apart from fraud, the NRA attaches a high threat level to corruption related offences committed in foreign jurisdictions. In addition, the NRA discusses threats posed by foreign tax crimes although this type of criminality has not yet been a subject to a ML prosecution in Liechtenstein. This notwithstanding, tax crimes are considered to pose a medium-high threat level.

Table 3.12: Foreign predicate offences

Predicate offences committed abroad	Level of threat
Fraud, criminal breach of trust and embezzlement	High
Corruption and active bribery	High
Tax offences	Medium-High
Narcotics offences	Medium

258. The predominant effort devoted to combating fraud committed abroad where proceeds were placed in Liechtenstein is largely in line with the highest assessed risk, but the situation is less clear when it comes to investigating or prosecuting non-fraud predicates assessed as high risks (such as ML linked to foreign corruption), medium-high (foreign tax crimes) and medium risks (trafficking in illicit drugs). The disparity between fraud and non-fraud cases (70% and between 5% to 30%) appears wider than the difference expected between their threat levels, even when qualitative factors (complexity, amount of proceeds, engagement of third parties, etc.) are taken into account.

Table 3.13: Investigations on predicate offences

Investigations for ML Predicate offences						
Year	Fraud	Theft and robbery	Corruption and bribery	Tax offences	Narcotic offences	Others
2016	67	5	5	3	3	6
2017	64	10	5	1	1	5
2018	36	17	10	2	4	8
2019	61	11	7	3	3	6
2020	78	6	13	5	7	12

259. Further to the threats analysis, the AT paid a great attention to the fact that Liechtenstein is an internationally networked and stable financial centre. Banks, asset and fund management companies, significant TCSPs sector, insurance undertakings, casinos and other financial intermediaries operate in the jurisdiction. The NRA states that *a significant inherent risk factor for all sectors arises primarily from the international customer base, which partly consists of countries with increased geographical risks, and which also includes a not inconsiderable number of PEPs. The characteristic services (wealth administration or private banking) inherently involve further risks because of the high level of assets involved, the influential clients, complex products and the expectation of confidentiality and discretion… A key attraction for the customer base described is the products and services offered by the TCSP sector. The establishment and administration of Liechtenstein legal entities, as well as of foreign legal entities, is one of the most important services or products on offer.*

260. These facts, in conjunction with cases presented to the AT and relevant statistical data, suggest that ML offences where e.g., TCSPs, who may have acted as professional intermediaries and concealed or made arrangements in respect of criminal property or failed to report their knowledge or suspicion of ML, should be a more common typology in the country. However, this and similar scenarios have rarely been a subject of ML investigations. Whilst some investigations/prosecutions involve financial intermediaries (e.g., cases where TCSPs committed fraud against their clients and then laundered these funds), majority of cases concerns self-laundering and ML charges against those who committed predicate offences.

261. As already noted, ML proceedings involving predicate offences committed abroad are considered by the authorities almost always as cases of autonomous ML. Authorities also advised that in autonomous ML cases, Liechtenstein is a mere transit country, i.e., the laundered assets came from abroad, are then laundered via one or more accounts in Liechtenstein and then sent to another country by means of transfers. The following cases provide more details on how this practice (which includes main risks/threats) has materialised.

Box 4 - Case studies

Case 1 –fraud

A German Prosecution Service had requested MLA in an advance fee fraud investigation where one of the suspects and recipient of a large amount of the fraudulently gained assets (two bank transfers of EUR 195 000 and EUR 125 000 to a bank in Liechtenstein) was still unknown. As a result of this information from the German authorities and of an analytical report of the FIU based on SARs/STRs an investigation for ML against the holder of the account of an establishment incorporated in Liechtenstein, a Danish national, was initiated in June 2014. In this investigation it was established that the BO of the bank account was the target of the investigation carried out by the German authorities. The evidence was shared with the German prosecutor who indicted the Danish national in February 2015 for serious fraud. The defendant was found guilty by the competent court in Germany in June2015 and sentenced to imprisonment of one year and ten months. In addition, property of corresponding value of the defendant was confiscated by the German court. In Liechtenstein, the suspect was charged with ML in September 2015. The indictment laid out how the suspect had hidden an amount of totally EUR 320 000 originating from the fraudulent activities in Germany in a bank account in the name of a Liechtenstein entity and how it was transferred to other accounts of third parties in Liechtenstein and abroad in 11 separate transactions. The trial took place in September

2016. The defendant pleaded guilty, and the court convicted him for stand-alone ML[17] of EUR 320 000. He was sentenced to 7 months of imprisonment for ML, in addition to 1 year and 10 months of imprisonment in Germany for the predicate offence. The execution of the sentence for was postponed for a probationary period of three years.

Case 2 – fraud

The suspect was the sole managing director of a Ltd. incorporated in Switzerland. He was also an authorised representative of a corporation in Liechtenstein. His accomplice was an accountant in a Switzerland corporation. In September 2013 they jointly arranged money transfers to be made by the Swiss corporation by means of fictitious or falsified invoices. The suspect issued fictitious or falsified invoices to the Swiss corporation on behalf of several different legal entities in the knowledge that these entities had no basis for these claims. The accomplice took the forged invoices to his workplace and entered the relevant legal entities as new creditors in the payment system and thus included the invoices in the payment run. Finally, the fictitious or falsified invoices together with the correctly recorded invoices on a due date list were released for payment. Among other invoices used in Switzerland, the suspect issued a fictitious invoice in August 2013 for CHF 178 200 to the Swiss corporation on behalf of the Liechtenstein corporation in accordance with the modus operandi described above. As a result, an amount of CHF 178 200 was transferred from an account of the Swiss corporation to the account of the Liechtenstein corporation with a bank in Liechtenstein. In September 2013 the suspect announced to the member of the Board of Directors of the Liechtenstein corporation the receipt of CHF 178 200 from the Swiss corporation. In order to check the plausibility of the receipt of the payment the suspect submitted the fictitious invoices dated. At the same time the suspect also presented a likewise fictitious invoice of a Swiss Ltd. to the Liechtenstein corporation for CHF 145 000, which was executed in September 2013 by transferring this amount to the account of the Swiss Ltd. with a bank in Switzerland. From this account the suspect withdrew the amount of totally CHF 145 108.35 in cash and handed over CHF 60 000 in cash to his accomplice. The accomplice and the suspect in Switzerland were found guilty in May 2016 for, inter alia, multiple fraudulent misuse of a data processing system and multiple forgery of documents (total damage CHF 468 206.30). In Liechtenstein the suspect was indicted for stand-alone ML in September 2016, in particular because he made false statements and concealed the origin of the CHF 178 200 by presenting the fictitious invoices to the member of the Board of Directors of the Liechtenstein corporation and because he transferred an amount of CHF 145 000 to the account of the Swiss Ltd. and withdrew this amount in cash. Due to the fact that the suspect is a citizen of Croatia who had no residence or stay in Liechtenstein, an international arrest warrant was issued in October 2018. The suspect was arrested in Switzerland in January 2019 and extradited to Liechtenstein. During the trial the suspect confessed that he committed the crime as described in the indictment and the court convicted him for autonomous ML. He was sentenced to 7 months of imprisonment. At the same trial, the member of the Board of Directors of the Liechtenstein corporation was heard as a witness. There was no evidence of his or other Board members' participation in the offence.

Case 3 – corruption in a foreign jurisdiction

[17] In this and in other cases described in boxes, the reader has to take into account the differences in AT's view on autonomous ML versus those of the Liechtenstein authorities, as expressed in the previous paragraphs under IO.7. In all these cases type of ML prosecution is expressed in line the authorities' qualifications of the case.

The suspect was found guilty of corruption and bribery by an Italian court in October 2013 and sentenced to 4 years and 6 months imprisonment. As a former commander of the municipal police the suspect was found guilty of accepting bribes and participating in a criminal organisation for carrying out official business in breach of his duties, in particular influencing the regional planning of the regional government. The suspect ensured the distribution of the bribes and brought his own share to Switzerland and Liechtenstein to cover up the traces. According to his confession in the Italian proceedings the suspect received EUR 97 500 to share this money with his accomplices. He opened a bank account in Switzerland and another bank account with a bank in Liechtenstein. The suspect paid the part of the bribe payments attributable to him into the account with the bank in Liechtenstein, claiming untruthfully to the bank that the money came from his professional activity as an independent consultant in the real estate sector. He transferred EUR 56 034 in December 2012 and EUR 1 354 in January 2013 to his account with the Liechtenstein bank and deposited EUR 8 728.12 in May 2013 in cash. On the basis of these findings and the conviction in Italy the suspect was indicted for stand-alone/autonomous ML in Liechtenstein in August 2014. The suspect pleaded guilty, and the Court of Justice convicted him for stand-alone ML of EUR 66 000 and forfeited this amount of money. Due to the value of the laundered assets the court did not impose an additional sentence (to the 4 years and 6 months imprisonment in Italy for the predicate offence) to the offender.

262. The cases discussed above are representative samples of ML investigations/prosecutions which involve the main ML threats as identified by the NRA. As already noted, tax crimes proceeds have not yet been a subject of ML prosecution in Liechtenstein. This issue was also analysed in the NRA, which states that *during the period 2016-2018, provisional inquiries relating to tax offences committed abroad were initiated in six ML proceedings, with approximately EUR 41.8 million being blocked. However, there were no charges or convictions.*

263. It is not uncommon that IFC are/have been used for tax evasion purposes. In that context, Liechtenstein is no exception. The country therefore undertook initiatives aimed at preventing the occurrence of ML where tax crimes would be a predicate. The most important of these initiatives are: (i) introduction of exchange of information in tax matters (in particular AEOI and FATCA) and corresponding disclosures or voluntary declarations, and (ii) disruption of money flows which would include tax saving and would usually go through one or more shell companies. With regard to the latter, the amendments to the CC introduced changes with regard to the ML offence and included tax savings as asset components subject to ML. This means that any banking transaction of these assets to third parties is considered to constitute ML pursuant to the amended Art. 165 (5) CC. Banks, their employees and management bodies could be held liable for ML if they transfer such assets to a third party. Banks have therefore adapted their policies and focused on domiciliary companies without economic substance as well as on commission payments without an economic background, since in these cases tax fraud can be assumed by virtue of regular use of forged or falsified documents. Banks now, de facto, regard business relationships involving the use of shell companies as means of tax optimisation and thus potentially classify them as tax fraudulent. For any business which includes banking operations, shell companies would have to provide evidence that an appropriate substance exists at the place of actual management and that the company makes economic sense. In the event that the requested proof cannot be provided, the banks would unilaterally take measures in the form of transaction blocks up to forced exit by account closure. Whilst the 2019 amendments

undoubtedly present a positive development in disrupting money flows deriving from tax offences, no criminal proceedings have yet been carried out as a result of Art. 165(5) CC.

264. On the other hand, the definition of tax offences is one of the reasons why there has been no ML cases related to this predicate so far. Only qualified tax offences (e.g., tax fraud which would involve forged documents) are defined as ML predicate offences, whilst simple tax evasion (regardless of the amounts involved) does not fall under this category. Other important factor is related to the mutual legal assistance in cases of tax offences. Due to the dual criminality principle, provision of mutual legal assistance in fiscal matters is possible only if an offence committed abroad would be a predicate to ML if committed in Liechtenstein. In other words, mutual legal assistance could not be provided for incoming requests which concern tax evasion only, neither the information they provide could be taken into account for ML investigation in Liechtenstein. The NRA noted that 11 MLA requests were refused in period 2016-2018, most of which included the cases of tax evasion. This notwithstanding, the MLAs in relation to serious tax offences (which are predicates to ML in Liechtenstein) are very rare and the authorities consider this fact as a main reason why no ML charges have been brought so far with serious tax offences being a predicate.

265. The AT discussed this matter in detail during the on-site visit and took into account the arguments raised by different interlocutors in Liechtenstein. It goes without saying that the results achieved in this area are not consistent with the risks/threats deriving from tax offences committed abroad. Whilst not disputing the right of each jurisdiction to decide, in line with its domestic legal principles, how to define each of the designated categories of offences and the nature of their particular elements, the AT believes that considerations should be given to broadening of the scope of tax offences so that it includes tax evasion. As discussed above, concrete actions undertaken to minimise the risks of tax offences' proceeds being laundered in Liechtenstein are welcome, however, the limitations related to the definition of serious tax offences hampers the authorities' efforts to further investigate ML stemming from foreign tax evasion. In addition, the AT is of the view that the FIU, OPP and the National Police appear to investigate foreign tax crimes reactively, rather than proactively in line with the medium-high level of risk and country's exposure as an IFC to foreign tax proceeds. In this context, the AT has some concerns as to why, for example, no asset holding vehicle established in Liechtenstein has ever been investigated as a potential mechanism for laundering the proceeds deriving from foreign tax offences. More efforts appear to be needed in this direction, including specialisation of the competent authorities to proactively investigate this criminality.

266. Other than these, the AT also discussed the risk related to cash and its integration in the financial system through FI, DNFBPs and VASPs. As discussed under IO.1 almost CHF 2 million is deposited and CHF 4 million withdrawn each working day in cash. The NRA provides little consideration of the use of large denomination bank notes, existence of cash intensive businesses, use of prepaid cards, handling of cash by TCSPs, or reasons for transporting cash cross-border. These typologies were not observed in any investigation/prosecution presented to the AT. Lack of such investigations and of proper analysis of this threat in the NRA do not provide sufficient grounds for the AT to conclude if the absence of typologies including cash is justified.

267. Overall, the types of ML activity being investigated and prosecuted are, to some extent, in line with country's threats and risk profile. Despite a relatively large number of ML investigations and pro-active approach by the authorities to pursue ML upon MLAs, the FIUs disseminations or

any other indication of a crime, large scale cases involving intermediaries/third parties do not yet present a considerable percentage in overall number of cases.

3.3.3. Types of ML cases pursued

268. Stand-alone ML (the way the authorities interpret it – see 3.3.1) is the most frequent type of ML prosecuted, followed by self and third-party laundering. In Liechtenstein, there is no need for the prosecution to prove the specific predicate offence in a ML case - proof of a ML act combined with evidence of reasonable grounds to believe that the property was criminal proceeds is sufficient. There are no particular difficulties in securing convictions in ML cases. It needs to be noted that in Liechtenstein, in ML proceedings, it has to be proven that the laundered assets are those that result from a criminal offence listed in the catalogue of predicate offences even if this predicate offence cannot be specified in more detail. In ML cases involving foreign predicates, the judges (in determining whether property is of a criminal origin and if the launderer is aware of this fact) are able to draw inferences based on objective factual circumstances. The evidence inferred from factual circumstances are often being obtained through MLA.

269. The ability to prosecute both self and third-party ML and to achieve convictions in standalone ML prosecutions was demonstrated to the AT with relevant statistics and ML case examples. These has also been discussed under 3.3.1 in relation to the overall number of convictions and the underlying predicates and the different types of ML cases. Speaking solely of investigations of ML, the authorities remain focused on simple and straight forward cases where the predicate has been identified abroad and notification on this was sent to Liechtenstein. This notwithstanding, judiciary has a sound understanding of what constitutes 3rd party and stand-alone ML offences and convictions achieved so far prove that their approach on this matter is compliant with what is required under criteria 3.5 and 3.8 of R.3. Judges are free to assess evidence and when they deem appropriate, they may also ask the defendants in ML cases to demonstrate the origin of assets concerned. This does not infer that the reversal of burden of proof is a principle which is applied in Liechtenstein, but that the judges may explore different areas in order to conclude if the offence was committed. In other words, discussions and cases presented assured the AT that there are no barriers to successful autonomous or stand-alone ML prosecutions and convictions.

270. Box below includes cases of different types/prosecutions of ML.

Box 5 - Case studies on different types of ML

Stand-alone ML

In 2012 a bank situated in the United States (US) became the victim of an orchestrated fraud-scheme, which capitalized on the shortcomings of the ACH (Automated Clearing House) system: Unknown perpetrators abused their account with the US-Bank by sending illegitimate debit requests from the US-Bank as the originating depository FI (ODFI) to other banks in the US as receiving depository FIs (RDFI). Upon receipt of the ACH requests, the RDFIs honoured the requests and transferred the funds to the account of an entity held at the US-Bank from where the funds were sent directly, in several tranches, to different accounts and FIs abroad with the aim to launder the money through further transfers and by using offshore companies. USD 266 000 was transferred into an account with a Liechtenstein bank held by a company

incorporated in the Seychelles. The BO of this company, a national of Bulgaria, tried to further launder the USD 266 000 by ordering the Liechtenstein bank to transfer the money into the account of another company with a bank in Canada. Meantime, the US-Bank had tried to validate the legitimacy of the debit requests as ODFI. The Liechtenstein bank learned that the debit requests were disputed by the costumers of the RDFIs whose accounts were improperly debited. Thereupon the US-Bank attempted to recall the outgoing international wires and informed the Liechtenstein bank that the transfer had been unauthorized and fraudulent. Hence the Liechtenstein Bank refused to transfer the money to Canada and filed a SAR/STR with the FIU. The defendant insisted that he had legitimately received the money and provided the Liechtenstein Bank with documents supposedly supporting his claim. Upon an analytical report of the FIU, investigation was launched, and the investigating judge issued a freezing order to the Liechtenstein bank. A participation of the defendant in the predicate offence could not be proven. An investigation by the FBI did not lead to any indictments or prosecutions of persons or entities for ML or fraud. Nevertheless, the defendant was indicted for stand-alone ML in Liechtenstein in March 2017 on the basis of circumstantial evidence. The suspect appeared in court and pleaded not guilty. The court nevertheless convicted him for stand-alone ML in August 2017. USD 266 000 on the account of the company incorporated in the Seychelles was forfeited. The suspect was sentenced to 12 months imprisonment.

Third party ML

In March 2013 a Liechtenstein bank transferred EUR 800 000 to various accounts in Albania and North Macedonia on the basis of forged transfer orders issued by unknown persons. Upon a complaint by a victim, the OPP initiated an investigation for fraud and ML against unknown and known suspects (the latter were account holders at banks in Albania and North Macedonia). Investigating judge issued seizing orders to the banks in Liechtenstein, Albania and North Macedonia. The seized banking documents from the Liechtenstein bank and the banking documents provided by the Albanian and North Macedonian authorities were analysed together with all the other transactions by the suspect with the Albanian bank: in March 2013 the suspect took EUR 57 950 originating from the fraud on a commercial basis committed by unknown perpetrators in Liechtenstein by withdrawing this amount from his bank account in cash in the following manner: he went to the bank and wanted to close his account. In doing so he was informed by the bank that there was an amount of EUR 57 950 on his account, which origin he allegedly did not know. Nevertheless, he withdrew this amount. Only transfers in relation to his account were his salaries amounting to approximately EUR 240. Participation of the suspect in the predicate offence could not be proven. The investigation for the predicate offence and ML against other two other suspects (account holders at a bank in North Macedonia) is still pending (unknown whereabouts), whilst the proceedings against two other suspects (account holders at a bank in North Macedonia) were closed due to lack of evidence. The suspect, owner of a bank account in Albania, was indicted for third party ML in Liechtenstein in February 2018. The features of this case clearly indicate that the indictment was based on circumstantial evidence where knowledge of the suspect is inferred from objective, factual circumstances. Since the suspect did not appear before the court in Liechtenstein, he was convicted in absentia for third party ML in September 2018. The court's decision stated that *dolus eventualis* by the suspect was proven by the prosecution and that the amount of EUR 57 950 on his account originates from crime committed by unknown offenders. The suspect was sentenced to pay a fine of CHF 1 000. No imprisonment sentence was imposed, and no assets were confiscated (no assets belonging to the accused were identified – he claimed that he had spent the amount concerned in gambling).

3.3.4. Effectiveness, proportionality and dissuasiveness of sanctions

271. As far as the legal framework is concerned, the ranges of sentences for ML for natural persons are as follows: (i) imprisonment of up to two years (Art. 165 (2) CC) and up to three years (Art. 165 (1) and (3) CC); and (ii) if the ML offence involves proceeds exceeding CHF 75 000 or is committed by a member of a criminal group associated for the purpose of continued ML, imprisonment from one to ten years (Art. 165 (4) CC). The courts can also impose fines. It is possible to impose fines in lieu of a penalty of imprisonment of not more than one year, if no sentence of imprisonment is needed to prevent the perpetrator from committing further offences (Art. 37 (1) CC). Sanctions for legal persons include fines that are calculated based on the gravity of the offence, the revenue of the legal person and a scale of daily rates (number of daily rates not more than 40 up to 180; daily rate is at minimum CHF 100 and at maximum CHF 15 000). There is no possibility for liquidation of the legal entity as a result of criminal proceedings, hence this can be achieved through parallel civil or administrative proceedings.

272. Whilst the legal framework provides a solid basis for sanctioning policy in the country, the cases presented and sanctions imposed so far suggest that their dissuasiveness and proportionality are not always assured. In cases where a predicate offence was committed abroad and the laundering took place in Liechtenstein, the judiciary determines sanctions as an addition to the sanction for predicate offence. In cases where ML was a concurrence offence to predicate, a single/cumulative penalty is imposed for the predicate offence(s) and for ML. Whilst imposing such penalties is in line with the national legislation ('one sentence for all crimes'), there is no clear indication how the ML component was weighted when these penalties were decided.

273. The additional penalties imposed for autonomous ML and the penalties for third party ML are in the lower area of the possible range of sentences. For example, in a case of third-party ML 12 months imprisonment was imposed for laundering of USD 266 000. Similar practice was observed in other cases. These sentences (see the table below) confirm the previous statement that they are not sufficiently dissuasive not proportionate.

Table 3.14: Imposed penalties

<table>
<tr><th colspan="3">Examples for imposed penalties (imprisonment) in ML proceedings</th></tr>
<tr><th>Self-ML
(overall penalty)</th><th>autonomous ML
(stand alone ML;
additional penalty)</th><th>autonomous ML
(third party ML)</th></tr>
<tr><td>8 years (6 years and 2 years additional penalty)</td><td rowspan="2">7 months (additional penalty to 1 year and 10 months)</td><td rowspan="4">12 months</td></tr>
<tr><td>6 years and 6 months</td></tr>
<tr><td>6 years and 6 months</td><td rowspan="2">7 months (additional penalty to 21 months)</td></tr>
<tr><td>5 years</td></tr>
</table>

4 years	6 months (additional penalty to 24 months)	
3 years and 6 months		
3 years	4 months (additional penalty to 2 year and 5 months)	

274. The assessment team also discussed sanctions against legal person. The case described in the box below is one of the examples when a legal person was held liable and fine being imposed. Arguably, the AT does not find the amount of financial sanction proportionate and dissuasive. Given the legal framework, it is evident that the impact of financial sanctions against legal persons varies and largely depends on legal person's size and financial assets it possesses. For institutions with significant assets, which number in Liechtenstein is not negligible, these fines are not proportionate or dissuasive.

3.3.5. Use of alternative measures

275. As discussed in previous chapters of this Immediate Outcome, there are no significant impediments or hindrances which make it difficult to achieve convictions in ML cases in Liechtenstein. On the other hand, problems related to obtaining information/evidence from abroad, which are often out of control of the jurisdiction and its authorities, and which exclusively depends on requested countries, may slow down and sometimes cause dropping of charges in ML cases initiated in Liechtenstein.

276. Liechtenstein introduced and has applied in practice criminal justice measures where, for justifiable reasons, ML conviction cannot be secured. These measures include (i) non-conviction-based confiscation – NBC (Art. 356 CPC); (ii) criminalisation of failure to report a suspicious transaction by a reporting entity (Art. 30 para 1 (a) of the DDA). These measures are frequently applied in practice. Whilst results of the NBC are discussed in detail under IO.8, the case in the box below provides details on application of Art. 30 para 1 (a) of the DDA.

Box 6: Case study demonstrating use of alternative measures

Two trustees and a trust company were indicted in March 2018 of having breached the duty of disclosure under Art. 17 (1) DDA from May 2016 to September 2017. The trustees as members of the board of directors of the trust company who were responsible for exercising due diligence obligations, did not notify the FIU in writing (submit a SAR/STR), despite an existing suspicion of ML or a predicate offence thereto. The two trustees were convicted in June 2018 (verdict confirmed in second instance in August 2018) following the indictment of breach of the obligation to notify pursuant Art. 17 (1) DDA for the offence defined in Art. 30 (1) (a) DDA.

They were fined to 120 daily rates both (one daily rate CHF 750 and 120, in total thus CHF 90 000 and 24 000). The execution of these sentences was postponed for a probationary period of three years. The trust company was also held responsible for the same offence committed by the both defendants (as board of directors of the trust company) and fined with 12 daily rates (one daily rate CHF 950) to a total fine of CHF 11 400. The execution of this sentence was postponed for a probationary period of three years.

277. As a matter of fact, Art. 30 para 1(a) of the DDA serves to charge those who fail to report suspicious transactions. Consequently, in cases where there are suspicions that persons subject to the DDA and their employees were involved in ML but where insufficient evidence was found to confirm this, Art. 30 para 1(a) of the DDA serves as an alternative measure to secure conviction. During the period 2016 – 2020, a total of 48 investigations were initiated under Art. 30 para 1 (a) DDA, 25 of which also included ML charges. First indictment under Art. 30 para 1 (a) of the DDA was brought in 2016 whilst in the period under review a total of 6 indictments against 11 persons (natural and legal) were issued. As a result, 5 persons (3 natural and 2 legal) are convicted.

Overall conclusions on IO.7

278. Liechtenstein's legal framework enables the effective detection, investigation, and prosecution of ML, including the ability to prosecute both self and third-party ML and to achieve convictions in standalone ML prosecutions.

279. Whilst ML investigations are prioritised and effective, prosecution and ultimately convictions do not follow this trend due to certain difficulties in obtaining evidence from abroad, the latter being the responsibility of jurisdictions where predicate offences were committed. The types of ML activity investigated and prosecuted are, to some extent, consistent with Liechtenstein's threats and risk profile and AML policies.

280. The cases investigated are managed effectively by smooth cooperation of the various authorities involved. However, Liechtenstein mostly investigates and prosecutes cases where the predicate offences (in particular fraud, corruption) were committed abroad and the illegally obtained funds subsequently brought to Liechtenstein by foreign offenders/criminals for laundering purposes. There are no prosecutions involving foreign tax offences as predicates, neither those where ML was committed through complex legal structures established in Liechtenstein, involving domestic financial intermediaries and/or shell companies. For successful investigations and prosecutions of such cases, the number of experienced staff in the various authorities involved might have to be increased (e.g., by forensic accountants and other economic experts).

281. The sentences imposed to both natural and legal persons cannot be said to be effective, proportionate and dissuasive since additional sentences for ML (based on existing foreign convictions) are rather low.

282. Thus, improvements are needed to enhance the effective investigation and prosecution of ML activities and the relevant sanctioning regime.

283. **Liechtenstein is rated as having a moderate level of effectiveness for IO.7.**

3.4. Immediate Outcome 8 (Confiscation)

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

284. Confiscation of criminal proceeds, instrumentalities and property of equivalent values is pursued as a policy objective in Liechtenstein. Legal and institutional frameworks are in place

(see related Recommendations in the TC Annex) and high-level commitment is ensured through several strategic documents.

285. An asset recovery policy was approved by the Government in November 2020. This policy document was prepared by the representatives of the Ministry for General Government Affairs and Finance, the FIU, OPP, Court of Justice, National Police and Office of Justice, then approved by the PROTEGE WG and consequently by the Government. The primary objective this document sets up is to deprive criminals and third parties from any benefit which derives from crime. It calls the competent authorities to exhaust all possibilities provided by law to attain this goal. This principle applies, in particular, to the offences committed abroad as these are considered to be of the highest risk.

286. Other objectives set up by the asset recovery policy aim at preventing criminal activities and their financing, no matter if they are done on an ad-hoc or a continuous basis. To achieve these objectives, law enforcement authorities, the OPP, the FIU and the competent courts are obliged to diligently apply the following principles: (i) *ensure strong and effective inter-agency cooperation*. To that end, parallel financial investigations must be carried out regularly; (ii) *ensure effective international cooperation* - considering the ML/FT threats/risks, effective international cooperation is a key to successfully trace proceeds and instrumentalities of crime. Competent authorities are therefore obliged to exhaust all cooperation channels with the aim to freeze/seize and then confiscate assets; (iii) *permanently examine and update measures in relation to the confiscation of proceeds of crime* – competent authorities are required to propose to the government legislative or other measures which are needed to promptly respond to the changing environment and risks the jurisdiction faces.

287. These policy statements have largely been materialised in practice through legislative reforms and through continuous strengthening of the institutional capacities. Amendments to the CC from June 2016 and October 2019 further strengthened the confiscation regime by, inter alia, introduction of the extended confiscation and confiscation of equivalent value (Art. 20 CC). Apart from assets under the control of a criminal/terrorist organisation and assets provided or collected for the financing of terrorism, extended confiscation is now applicable to: (i) any asset which could be connected to the perpetrator are also subject to extended confiscation if there is a reason to believe that they derived from an unlawful act and if their lawful origin cannot be substantiated; (ii) if ML, organising a criminal/terrorist group, or other terrorist or corruption related offences have been committed in a continuous or a repeated manner, any assets suspected to be connected with these offences which lawful origin cannot be substantiated, are subject to extended confiscation.

288. In addition, Liechtenstein introduced a non-conviction-based confiscation. If the results of the criminal proceedings do not suffice in themselves, the court may issue a ruling to the effect that the decision on confiscation is discussed in a separate proceeding (Art. 356 CPC). If there are sufficient grounds for the assumption that the conditions for confiscation/extended confiscation are met, and if it is not possible to decide on this in the criminal proceedings against a specific person, the prosecutor has to submit a separate application for non-conviction-based [in rem] confiscation. This application must specify the object(s) or asset(s) affected by the order, the criminal act on which the order is based, as well as the liable party(ies).

289. The OPP and the National Police are in charge for financial investigations, the basis of which was discussed under IO.7.

290. The National Police, being a leading law enforcement institution in tracing, seizing, freezing, and ultimately confiscating the proceeds of crime benefits from its long experience in executing these tasks. Their internal instructions indicate steps that need to be taken in the course of financial investigations including databases checks and communication with national authorities (such as the FIU and tax administration) and foreign counterparts. The "Guidelines on pecuniary orders in Liechtenstein law" are specifically tailored for financial investigators and provide a detailed overview of all measures available to secure and confiscate the proceeds of crime. It also helps practitioners where to look when seeking/detecting/tracing criminal assets, including the assets moved abroad. These guidelines were developed as a response to the requirements of the UN Convention against Corruption, and they have been published at the homepage of the StAR Initiative. The OPP, National Police and investigative judges regularly attend the trainings in the country and abroad where confiscation related matter are discussed. The AT also noted that the competent authorities attended trainings related to confiscation of VAs, one of the areas which is very material for the jurisdiction. Whilst all police officers are trained to carry out simple financial investigations, complex and labour-intensive cases are carried out by the Crime Investigation Division of the National Police and its Financial Crime Unit. There are eleven officers dealing with financial investigations in complex cases.

291. The confiscation policy applied in Liechtenstein, analysed in conjunction with the investigative actions, seizures/freezing and confiscation executed so far (in the country and abroad – please see core issue 8.2) clearly indicate that the country has a policy objective to use the widest range of tools and mechanism to prevent and deter benefits from criminal activities.

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

292. The Liechtenstein courts routinely order the confiscation of assets previously seized/frozen over the course of a criminal investigation. The burden of proof is on the OPP who, by presenting and elaborating the evidence gathered, needs to prove that the proceeds originate from criminal activity. The court then decides, when pronouncing a judgement, whether or not to approve the confiscation. The Court of Justice is also a competent authority for responding and for requesting information and evidence to/from foreign counterparts which concern tracing and identification of proceeds of crime.

293. To begin to consider how well a jurisdiction identifies proceeds of crime, information is generally needed on the overall numbers of detected proceeds-generating offences, and the numbers of parallel financial investigations opened in such cases, for comparison. Such comparison, however, might have been difficult in a jurisdiction where confiscation measures are applied against predicate offences which were predominantly committed in foreign jurisdictions. From the information provided by the authorities it would appear that pro-active parallel financial investigations have been developed and pursued persistently over the period under review.

294. The exact figures on financial investigations carried out by the National Police, with or without prior instruction by the OPP or investigative judge (for the period 2016 to 2019), are: 2016 - 68; 2017- 49; 2018 - 49; and 2019 – 70. Compared to 343 ML investigations initiated during the same period (see table under C.I. 7.1), the total number of 236 financial investigations involving National Police confirms the approach by the competent authorities (i.e., the OPP and

investigative judge) that not all ML investigations require engagement of the National Police. This issue was discussed with the competent authorities – the reasons behind stand with the fact that in some ML cases no additional investigative actions by the National Police were considered needed. Consequently, the figure presented under IO.7 includes all financial investigations with or without the involvement of the National Police.

295. Another element which is advantageous for the confiscation regime in Liechtenstein is the fact that for seizure and freezing orders to be approved a suspicion that proceeds derive from crime is sufficient. This has been confirmed by the Constitutional and Supreme Court decisions (decisions from 2016 and 2019). As an example, an analytical report by the FIU, where there are grounds for suspicion that proceeds are of a criminal origin, is sufficient for the court to grant a freezing/seizure order. The court has to lay down a period of time not exceeding two years for which the freezing order will be valid. On application of the OPP, this time limit may be extended – such extensions are given for a year's time. However, there is no limitations on how many times these extensions could be given in a particular case. On the other hand, the case law suggests that these orders are not to be prolonged after three years' time unless investigation results substantiate the initial suspicion. Prolongations are also limitless if an indictment has been submitted or if a conviction, albeit not yet final, has been rendered. In such cases, extensions of up to ten years and beyond are possible. Freezing/seizing orders may also be lifted or not renewed prior to the expiration of the time period of three years in cases where a vague initial suspicion has not been substantiated.

296. The vast majority of assets seized/frozen in Liechtenstein are funds on bank accounts. A trigger for a request for freezing is, in most of the cases, a SAR/STR filed to the FIU. The FIU's temporary freezing order may then be used (see IO.6). This administrative measure may last up to 48h, a period during which the OPP may request and get approval from the court for a judicial freezing measure to be applied to the amount(s) concerned.

Year	Amounts frozen/ property seized (EUR)	Property confiscated (EUR)	Property effectively recovered (EUR)
2015	169 513 447	5 604 625	5 604 625
2016	82 018 552	1 687 803	1 687 803
2017	121 715 609	5 463 475	5 463 475
2018	525 301 541	1 972 315	1 838 815
2019	528 252 841	44 170 816	22 664 238
2020	155 567 405	6 255 815	5 567 585
Total	1 582 369 395	65 154 849	42 826 541

297. As it may be observed from the table above, the amounts seized/frozen and confiscated are considerable. Overall, EUR 1 582 369 395 was seized/frozen whilst EUR 65 154 849 was confiscated, and EUR 42 826 541 effectively recovered in the period 2015-2020. The AT also observed that the amount of the confiscated assets is still far inferior to the sums seized/frozen. The authorities advised that the amount of confiscated assets is expected to increase significantly once the on-going investigations and subsequent court proceedings are completed. In their view, this gap primarily resulted from sometimes slow MLA/information exchange procedures. Given the discussions on evidence gathering in cases where an international cooperation is included

(see IO.7), this reasoning seems adequate as no other impediment in this regard was observed by the AT.

298. Authorities were also able to demonstrate that they confiscate the *property of equivalent value*. As a matter of statistics and case law presented, it appears that this component of the confiscation regime is frequently applied in practice. This has particularly been the case since 2018. The case below provides an example of such confiscation.

Box 7: Case studies on confiscation of criminal proceeds

Case 1: Following the criminal complaints filed by clients of Liechtenstein trustees, investigation was carried out by the National Police and the investigating judge upon request of the OPP in April 2018. Offences allegedly committed by two suspects included fraud, criminal breach of trust, embezzlement and self-ML. Further to several house searches and seizure of numerous documents at different banks, the FIU submitted several analytical reports to the OPP. In December 2018 the defendants were charged for fraud, criminal breach of trust, embezzlement and self-ML. In summary the first defendant was accused of abusing his authority as a representative of eleven legal persons and of having used a total of more than CHF 21 million without the knowledge of his clients (criminal breach of trust), deceiving several persons and causing damage to three natural and legal persons of more than CHF 1.8 million (fraud) and for embezzlement of about CHF 80 000. The second defendant was accused of abusing his authority as a representative of six legal persons and of having used a total of more than CHF 3.5 million without the knowledge of his clients (criminal breach of trust) and for embezzlement of CHF 50 000. Consequently, the defendants were convicted for fraud, criminal breach of trust, embezzlement and ML and sentenced to 6 years and 6 months and 2 years and 6 months of imprisonment. At the trial held in July 2019 a settlement between the first defendant and the injured parties to pay damage of more than CHF 23 million was reached. Because of this settlement forfeiture of this amount was excluded (Art. 20a (2) CC). In addition, the assets of the defendants in the amount of CHF 2.15 million as property of corresponding value were confiscated pursuant to Art. 20 (3) CC. In total CHF 2.8 million were confiscated. Whist at the appellate proceedings the imprisonment sentences were reduced, the confiscation order was declared final.

Case 2: ML proceedings against three German nationals were initiated in December 2010. Around EUR 196 000 which originate from a fraud were transferred to an account of a Liechtenstein corporation with a bank in Liechtenstein. The remaining assets at this account (CHF 69 000) were frozen following an MLA-request from Germany. All suspects had been convicted for the predicate offence in Germany. Pursuant to the then Art. 165 (5) CC, which was cancelled meanwhile, a person at that time was not liable for ML if he/she was punished for participation in the predicate offence. Because no confiscation order from Germany (in addition to the MLA request for freezing) had been received, non-conviction-based proceedings were initiated in November 2017. An application for confiscation of EUR 196 000 was filed by the OPP in March 2018. In a judgement handed down in Germany, the Liechtenstein corporation was found to have received EUR 196 000 obtained through a criminal offence (fraud committed in Germany). The assets of Liechtenstein corporation were then confiscated by a judgment of the Liechtenstein criminal court (in May 2018 it became final). The judgements states that around CHF 69 000 frozen at the corporation account was confiscated as a direct proceed of crime/laundered property, whilst for

the difference amounting up to EUR 196 000 the court imposed the confiscation of the monetary equivalent.

299. As discussed above, non-conviction-based confiscation is also an instrument which Liechtenstein authorities continuously apply in practice. The cases concerned mostly include confiscation from unknown perpetrators or perpetrators who do not reside in Liechtenstein and whose whereabouts are unknown. The table below presents a breakdown of conviction and non-conviction-based confiscations.

Table 3.15: Conviction and non-conviction-based confiscations

Assets confiscated						
Year	Total		conviction-based		non-conviction-based	
	cases	amount (EUR)	cases	amount (EUR)	cases	amount (EUR)
2016	5	1 687 803	3	1 057 631	2	630 172
2017	8	5 463 475	6	1 056 805	2	4 406 670
2018	10	1 972 315	6	1 606 465	4	365 850
2019	14	44 170 816	12	44 058 046	2	112 770
2020	15	6 255 815	11	5 700 575	4	555 240

300. The number of cases and amounts confiscated so far as a result of non-conviction-based confiscation confirm that the authorities regularly use this mechanism in practice. Discussions held on-site also confirmed that the authorities are aware of the importance of this instrument's application given the risk and context of the jurisdiction in this area.

301. Another example of non-conviction-based confiscation is presented below:

Box 8 - Case study on non-conviction-based confiscation

With the verdict of an Italian court of April 2015 the two suspects were found guilty of fraud in the payment of excise tax duties in connection with the trade of high-quality wine. The first suspect was sentenced to two years imprisonment, with the execution of the prison sentence being suspended while the second suspect got a prison sentence of three years. In summary this conviction is based on the facts that the two suspects transported wine from Italy to England from May 2012 to April 2013, but relevant customs documents did not indicate neither the quality nor the quantity of the wine delivered, whereby excise tax duty in England was evaded in the amount of more than EUR 9.6 million. The transport of the wine was executed by different transportation companies. On the return journeys the drivers brought large sums of cash so that the proceeds from these criminal acts could flow back to the perpetrators. Between May 2012 and April 2013 incriminated funds of about EUR 158 000 were paid in cash and transferred to an account of a corporation at a Liechtenstein bank. BOs of this account/corporation were the two suspects. They also transferred GBP 133 791 in July 2012 to an account of a Trust at the same bank. Italian authorities, in course of their financial investigation traced these amounts and established that the amounts in the accounts of the corporation and the Trust at the Liechtenstein bank originate from the illegal activities. The case against the two suspects for ML in Liechtenstein was dropped for evidentiary reasons in

April 2019; however, non-conviction-based proceedings were initiated. An application for forfeiture of EUR 302 700 was filed by the OPP in January 2020. As a consequence, the court ordered EUR 148 000 from the account of the corporation and EUR 154 700 from the account of the Trust to be confiscated.

302. As it was noted under CI 8.1, extended confiscation is one of the mechanisms available to Liechtenstein authorities to deprive criminals from keeping assets which could be connected to their criminal activities. Whilst this mechanism exists since 2016 (with amendments made in 2019), the AT finds it somewhat difficult to establish to what extent the authorities succeeded to confiscate assets that go beyond the direct proceeds of a concrete criminal offence for which the defendant is prosecuted. The authorities argued that they always look into the financial profile of the suspect/defendant, check tax authorities reports on incomes declared and also, during a house search (if this measure is carried out for confiscation or evidence gathering purposes) objects of a significant value would be noted and considered as a potential subject of extended confiscation. However, these statements and clear awareness of the competent authorities of opportunities provided by the law, including the one case presented to the AT, were not sufficient to confirm that this mechanism is frequently applied in practice. As regards the relative materiality of this issue on the overall confiscation results, the AT is of the opinion that, due to the specific context of the jurisdiction (i.e., priority given to confiscating the laundered property) this issue has not had a major impact. This notwithstanding, more attention needs to be paid on this aspect of the confiscation regime, including more concrete guidance and training predominantly for the law enforcement authorities.

Confiscation from third parties

303. Confiscation from third parties involves cases where the third parties knew, or should have known, on the basis of concrete facts, that the transfer was intended to avoid confiscation. In Liechtenstein, confiscation from third parties is possible in both conviction and non-conviction-based proceedings. Third parties have to be involved in these proceedings as *jointly liable persons*, i.e., natural or legal persons who - without being accused themselves – are in possession of item(s) subject to confiscation. They have the rights of a defendant in the trial and in appeal proceedings as far the decision on confiscation is concerned. Authorities advised that when natural or legal *persons who knew that the transfer of assets intended to avoid confiscation* are always investigated and indicted for ML. In other words, all ML related confiscations that involve third parties, in their view constitute this type of confiscation. Arguably, the effectiveness in relation to confiscation from third parties should take into account this contextual factor. On the other hand, cases where third parties 'should have known that the transfer was intended to avoid confiscation' are not considered as ML offence in Liechtenstein given that ML requires firm knowledge of the third party on the origin of assets. Consequently, confiscation from third parties where no ML charges are included are not frequent. This notwithstanding, the authorities remain vigilant to these possibilities especially when it concerns assets transferred to legal persons established in Liechtenstein. Two such cases were presented to the AT where confiscation from third parties (these being legal persons) were ordered by the court.

Instrumentalities

304. Whilst the proper legal framework is in place for confiscation of instrumentalities, this component of the overall confiscation regime in Liechtenstein appears less material given the nature of the offences which are subject to investigations/prosecutions. As already discussed, predicates such as fraud or corruption do not require specific instrumentalities. Understandably, there are no statistics available for confiscation of instrumentalities. Authorities presented several cases where some narcotics dealing equipment (grinders, mobile phones and cars used in the management of drug trafficking) was confiscated. Given the (little) materiality of this component of the confiscation regime, the AT does not consider this to be an issue.

Seeking assets abroad

305. Seeking assets abroad appears to be somewhat difficult for Liechtenstein law enforcement and the OPP given the fact that criminal assets are, in vast majority of cases, generated abroad, sometimes these assets only passed through the Liechtenstein FIs and are then redirected to foreign jurisdiction(s). When MLA requests to other countries to trace, secure (freeze and seize) and forfeit assets or confiscate instrumentalities are sent, the usual practice is that the FIU initiates informal information exchange with its foreign counterparts for purpose of locating the assets (i.e., funds). Other inquires include communication via the CARIN network and police to police bilateral information exchange. Interviews held on-site confirmed that when an MLA request for freezing assets abroad is sent, some jurisdictions (excluding here the neighbouring countries) need a considerable period of time and by then the funds may already be gone. These issues do not infer that Liechtenstein authorities are not pro-active in seeking assets abroad. By contrast, discussions held onsite, and several cases presented to the AT (including tracing and freezing assets in Italy, Portugal, Austria) confirmed the pro-active approach by the authorities on this component of the confiscation regime.

306. As a matter of legislation, assets confiscated by a decision of a Liechtenstein court become a property of the jurisdiction. The Government is also entitled to decide on assets sharing with foreign counterparts. Prior to any such decision, the Office of Justice prepares a file where relevant information is gathered and upon which the Government may decide. Asset sharing is done on a case-by-case basis. The same approach is applied when requesting foreign counterparts for repatriation of assets to Liechtenstein.

Below are the figures which indicate how assets were shared in the period 2016 to 2020:

Year	assets forfeited subject to sharing (EUR)	shared assets sent abroad (EUR)	shared assets that stayed in Liechtenstein (including costs)
2016	1 718 982	848 497	870 465
2017	501 107	487 471	13 636
2018	2 015 293	966 135	1 049 158
2019	270 877	172 727	98 150

2020	18 965 848	18 386 853	578 995

307. Compensation of victims in confiscation proceedings is another aspect the authorities take into account. Several case studies have been presented to the AT. These cases included victims' compensation in the country and abroad. Given the predominant presence of fraud as an offence which proceeds are subject to confiscation, Liechtenstein authorities developed good knowledge and understanding of giving considerations to returning the confiscated property to the victims of crimes.

308. Liechtenstein does not have a single-purpose authority in charge of managing seized and confiscated assets. Assets frozen/seized are under judicial custody until the proceedings come to an end. Frozen assets remain frozen at the bank account and the account holder needs an approval of the court if he/she wants to make any investment with these assets. Other than funds, authorities keep seized assets at the Court of Justice or at the National Police. Immovable property, such as real estate, remain in possession of the defendant but his/her rights regarding the property's disposition are under judicial prohibition until the proceedings are over. Given the nature of assets confiscated in vast majority of cases in Liechtenstein (i.e., funds on bank accounts), the AT is of the opinion that the current framework is adequate and provides solid basis for asset management. If, however, the environment changes and cases where complex assets are seized (e.g., businesses, specific goods which value may deteriorate quickly, pieces of art, etc.) become frequent, the authorities should consider either a setting up of a single-purpose authority for asset management or establishing a unit of asset management specialists which would be attached to one of the existing institutions. In this context, several new provisions have been introduced: starting from July 2021, the legislation provides new possibilities for alienation of assets seized which are subject to rapid deterioration or considerable depreciation in value or can be preserved only at disproportionate cost; new possibilities are also introduced for collection or alienation of frozen funds, monetary claims, and transferable securities.

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

309. Confiscation of falsely or undeclared cross-border transaction of currency/BNI is a sui generis case in the evaluation of Liechtenstein. Based on the framework treaty with Switzerland on police cooperation in the border area and the associated execution and implementation agreements, the National Police has delegated its cash control powers to the Swiss Border Guard Corps (see R.32). The Swiss Border Guard Corps is empowered to carry out cash controls along the Liechtenstein border with Austria and to apply the Swiss Border Guard Corps' regulations in that regard. Switzerland and consequently Liechtenstein apply a disclosure system. Whenever a disclosure is made at Liechtenstein cross border points with Austria, the information is immediately transmitted to the National Police. In case of false or lack of disclosure (including when there are suspicions of ML/TF), the National Police would immediately be called to come to the border crossing point and be present during any investigative activity. The FIU would be immediately notified, too. The case below is the one where cash was restrained due to ML suspicions. It also shows a modus operandi applied in such situations.

Box 9 - Case study

A Chinese national was controlled by the Swiss Border Guard Corps at the Austrian – Liechtenstein. He was asked about the cash he was carrying. He declared that he was carrying cash in the amount of approximately EUR 5 000. During the baggage check approximately EUR 1 200 and CHF 7 000 were found. Vehicle search revealed an additional amount of EUR 50 000 Subsequently the National Police was informed by the Swiss Border Guard Corps. The National Police initiated inquiries against the Chinese national for ML as well as for the infraction pursuant to Art. 36 para 2 Police Act (false information at a cash control). The National Police also restrained the cash found by the Swiss Border Guard Corps and after the interrogation of the suspect reported the case to the OPP. Suspicious activity report was immediately filed to the FIU. The OPP initiated a ML investigation whilst seizing of cash was approved by the court. Investigation could not prove that the cash originated from crime and was thus closed. The Court of Justice convicted the suspect for the infraction pursuant to Art. 36 para 2 Police Act and imposed a fine of CHF 10 000. After the amount was paid, the seizing order was lifted.

310. The AT was also informed that the National Police carry out additional controls close to the border to Austria and/or Switzerland. These controls are exercised by the Security and Traffic Division or by the Crime Investigation Division (with or without support of the Swiss Border Guard Corps) and they target cash curriers. Regardless of the results of these controls (e.g., if there are suspicions that ML/TF /predicate offence were committed), the National Police make record of each control undertaken and keep it in their database (date of the control, place, findings, etc.). Even when no suspicions are recorded, the National Police provide, on annual basis, the FIU with statistic on all cash controls they carried out. In the period 2017-2021, 56 controls were made, out of which 3 triggered a suspicion and were immediately shared with the FIU.

311. Information provided within this core issue sheds some light into the cross-border regime and its effectiveness in restraining illicit cash flows. However, the AT faced certain difficulties to fully assess this component of the confiscation regime. The reasons are manifold: (i) responsibilities are entrusted to another jurisdiction (Switzerland), so the Liechtenstein authorities' actions largely depend on the effectiveness of controls carried out by the Swiss Border Guard Corps; (ii) other jurisdiction's MER's findings vis-à-vis this core issue indicate that 'little information is available on the confiscation and sanctions imposed in connection with cross-border cash transfers' (Swiss MER, page 73) – it is unclear to what extent this should be a factor when assessing the same core issue for Liechtenstein; (iii) the AT met the Swiss Border Guard Corps during the on-site visit and, further to the discussions held with them, can only reaffirm some of the finding of the Swiss MER; (iv) statistics concerning the border points covering Liechtenstein are available and indicate very few cases of cash disclosures.

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

312. Given the fact that the majority of cases where confiscation measures are applied include a ML component, the analysis provided under core issue 7.2 is valid here. In addition, considerable amounts were confiscated as a result of foreign countries' decisions and as per incoming MLA requests. In these cases, predicates such as tax fraud also feature in (together with other high risk predicates such as fraud/embezzlement/breach of trust, corruption and drug

trafficking), thus substantiating the conclusion that the confiscation results generally do reflect the assessment of risks and the national AML/CFT policies and priorities.

Overall conclusions on IO.8

313. Liechtenstein pursues recovery of criminal proceeds, instrumentalities, and property of an equivalent value as a policy objective. Results achieved during the period under review are substantial – significant funds were confiscated and even more significant have been seized pending the final court decisions. Competent authorities (the OPP, investigative judges and the National Police) have demonstrated their strong capabilities in pursuing direct proceeds of crime as well as the property laundered. Consequently, the value of assets recovered in relation to foreign predicate offences represent a significant percentage of the total value. Non-conviction-based confiscation is frequently applied, which, given the context of the jurisdiction, presents an important feature of the overall confiscation regime. Some components of the confiscation regime are still in need of improvement – primarily the application of the extended confiscation (as per Art.20(2) b of the CC) and the cross-border confiscation of cash.

314. Confiscation results are generally in line with the risk profile of the jurisdiction.

315. **Liechtenstein is rated as having a substantial level of effectiveness for IO.8.**

4. TERRORIST FINANCING AND FINANCING OF PROLIFERATION

4.1. Key Findings and Recommended Actions

Key Findings

Immediate Outcome 9

a) Liechtenstein's legal framework to fight TF is broadly in line with the international standards. Being geographically located between Switzerland and Austria, Liechtenstein closely cooperate with these countries for combatting terrorism and TF. Extensive relations with the relevant counterparts in Switzerland, Austria and Germany are in place with several information exchange platforms being used.

b) There have been no TF prosecutions/convictions in Liechtenstein so far. One TF investigation was carried out, but it did not result in further proceedings as no evidence of TF was found. This notwithstanding, the features of this case and actions undertaken by the competent authorities confirmed that they are equipped with skills and knowledge on how to detect collection, movement and use of funds for TF purposes. The absence of TF prosecution is generally in line with the country's risk profile.

c) The country has never received an MLA request from foreign counterparts in relation to terrorism or TF. The TF risk assessment concluded that the risk of TF in Liechtenstein is medium. Whilst the AT finds the conclusion on the level of TF risk as reasonable, further efforts need to be invested in analysis of transactions with high-risk jurisdictions and appropriateness of SARs/STRs reporting on this matter.

d) Since there have been no prosecutions/convictions for TF, no conclusion could be made on proportionality and dissuasiveness of sanctions applied. On the other hand, sanctions, as envisaged by the CC for the TF offence, appear proportionate and dissuasive.

e) Whilst there is no specific counter-terrorism related strategy developed by the country, the initiatives taken by Liechtenstein in the field of CFT show an appropriate degree of commitment, inter-agency cooperation and awareness by the competent authorities. The country developed a TF Strategy targeting its main goals in developing its ability to prevent/suppress TF. The Strategy is followed by concrete actions by the FIU and the National Police which developed specific documents/instructions for their officers on how to investigate TF.

f) Although some measures to disrupt TF are available to the competent authorities (such as expulsion of foreigners as per the Foreigners Act) none of these has yet been applied in lieu of proceedings with TF charges.

Immediate Outcome 10

a) Liechtenstein has a sound legal framework which ensures automatic implementation of relevant UNSCR covering TFS into the national framework. Amendments introduced in 2020 and 2021 set the competent national authorities and relevant procedures, in particular with regard to supervision and designation/listing/de-listing, parts of which have been

implemented recently, thus the level of their effective implementation could not be fully assessed for these parts.

b) Liechtenstein competent authorities, under the coordination of STIFA, have undertaken a NPO risk analysis aimed at identifying the subset of NPOs falling under the FATF definition and representing a high risk for TF, as well as revealing possible typologies on their misuse for TF purposes. Residual risks for foundations and establishments were assessed as moderate-low, and low for associations.

c) Monitoring/ supervision over foundations and establishments is conducted through several authorities, including the FMA (AML/CFT supervision on due diligence obligations for TSCPs acting as qualified members of the governing body of the NPO), STIFA (on the consistency of expenditure with the primary purpose) and the Fiscal Authority. As for associations, at the moment they are subject to fiscal supervision. Certain measures have been implemented in relation to this sector, however those do not amount to TF risk-based supervision/monitoring. This notwithstanding, the NPO Risk Report was a trigger for additional oversight measures regarding NPOs identified as "high-risk".

d) Awareness raising has been conducted through training, meetings and fact sheets delivered to foundations and establishments. Those met onsite were aware of the NPO Risk Report results and had a good understanding of the risks they might be exposed to. This cannot be attributed to associations. The association met onsite was not aware of the obligations vis-a-vis CFT measures and the ways associations could be misused for TF.

e) Several false positive matches to lists have been filed with the FIU, however none of them was confirmed to be a true match. There has been no freezing, as well as confiscation of assets so far.

g) Measures undertaken by the competent authorities are consistent with the jurisdiction's overall TF risk profile. There have been no NPO-related information requests from foreign competent authorities or confirmed cases. At the same time, the authorities were able to demonstrate - through actions taken in relation to other sanctions regimes - that in case of a real TF case they would be capable of taking action consistent with the requirements under respective UNSCRs.

Immediate Outcome 11

a) Measures in place aimed at implementation of PF related TFS are identical to the ones related to TF TFS.

b) Awareness and understanding on PF related TFS and respective obligations is generally good among persons subject to the DDA, while the banks and some TCSPs demonstrated better understanding in this regard. Some of the smaller FIs and DNFBPs do not clearly distinguish between TF and PF TFS. Most persons subject to the DDA screen against all UN lists on automatic checks for UNSCR updates, relying on commercial databases. Shortcomings examined under IOs 4 and 10 in this regard are also applicable for PF TFS screening.

c) Liechtenstein has not frozen any assets or transactions as a result of PF-related TFS. There are no PF-related SARs/STRs. Persons subject to the DDA have filed several ISA reports with

the FIU on potential sanctions evasion unrelated to PF TFS, which demonstrates ability to take action in case of a potential PF related case.

d) Supervision on implementation of PF TFS has just recently been introduced, thus not being in place for the most period under review. FMA and Chamber of Lawyers are the authorities designated to carry out this supervision. While the FMA has already practiced targeted TFS related inspections, the Chamber of Lawyers does not have any prior experience in this area. In addition, the FIU acts as the ISA authority, having the power to investigate potential sanctions evasion cases.

Recommended Actions

Immediate Outcome 9

a) The authorities should continue with their analyses of financial inflows and outflows from high-risk jurisdictions, seek further cooperation by these jurisdictions in identifying potential TF suspicions and continuously analyse the appropriateness of SAR/STR reporting by FIs, DNFBPs and VASPs on this matter.

b) National Police and the OPP should, within the framework of their on-going trainings on TF investigations, include the components on emerging techniques used for TF, primarily the TF typologies which include VAs.

Immediate Outcome 10

a) Liechtenstein competent authorities should ensure effective application of the recently introduced legal framework, through issuing relevant procedures/instructions aimed at identification of targets for designation/ listing, processing of incoming requests, processing of outgoing requests related to freezing of funds, de-listing, and granting exemptions, as well as by clarifying their respective roles and responsibilities in these processes.

b) The competent authorities should conduct further outreach to FIs, DNFBPs, and VASPs in relation to their compliance with obligations under the FT-related TFS regime, including on newly developed guidance, the reporting regimes to be used, as well as the scope of persons towards whom TFS should be applied. Persons subject to the DDA with less developed understanding should be the primary focus of these initiatives.

c) Competent authorities should invest further efforts aimed at introduction and enforcement of risk-based monitoring/supervision for all NPOs representing a high risk for TF (as identified by the NPO Risk Report), also including associations. Further awareness raising initiatives should be undertaken for associations, including through outreach and/ or guidance to those entities and the donor community, with a focus on possible risks of being misused for TF and applicable CFT measures in this regard. This should however be done in a way not to disrupt the legitimate activities of associations.

Immediate Outcome 11

a) As in case of TF, the authorities are invited to invest further efforts aimed at full implementation and effective enforcement of the newly introduced/ amended framework through introduction of further guidance, clarification of respective roles and increased supervision for all the private sector representatives.

b) Authorities should ensure that appropriate training is delivered to all supervisors (including commissioned auditors and Chamber of lawyers) to enable consistent targeted TFS supervision among all the sectors.

c) Further PF TFS specific guidance and training should be provided to persons subject to the DDA, with a specific focus on small FIs, VASPs and DNFBPs, including on their PF TFS related obligations, reporting regimes, scope of persons towards whom the TFS should be applied, including indirect ownership and possible typologies.

d) PF TFS related supervision should continue to be a part of the activities of the FMA in the framework of onsite inspections. The latter should include the verification of compliance with such obligations, by, *inter alia*, ensuring, that the screening of entities against the UN sanctions lists includes entities already existing in databases of persons subject to the DDA and assets are frozen where necessary. PF-related TFS should also form part of the supervisory activities of the Chamber of lawyers during the on-site inspections.

316. The relevant IOs 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, and elements of R.2, 14, 15, 16, 32, 37, 38 and 40.

4.2. Immediate Outcome 9 (TF investigation and prosecution)

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

317. There have been no TF prosecutions/convictions in Liechtenstein so far. One TF investigation was carried out, but it did not result in further proceedings as no evidence of TF was found (see core issue 9.2). Liechtenstein authorities has never received MLA request on TF. The AT considers that the lack of prosecution is, generally, in line with the jurisdiction's risk profile.

318. Liechtenstein closely cooperates with the neighbouring countries (Switzerland, Austria, Germany) in addressing the threat of terrorism and FT. The National Police and the FIU maintain links with various partners and stakeholders from these countries' networks (counter terrorism and intelligence), as well as with any other national authorities if need be.

319. Liechtenstein has never experienced a terrorist attack in its history. Demographic and geographical factors pose a low risk of domestic terrorism. A third of the population of Liechtenstein are foreign nationals, mainly from Switzerland, Austria, and Germany. The country has no parts of its population that would be sympathetic to the terrorist cause. The authorities advised that there is no information which would indicate that any terrorist organisation operates in or has any links to Liechtenstein.

320. Although there is always a risk of radicalisation of individuals in any population, there is no intelligence that there is a problem with so-called foreign terrorist fighters and the funding of such fighters. The National Police has access to the FTF Interpol database, the FIU is empowered to request information from persons subject to the DDA even in absence of an SAR/STR being submitted, allowing for a dynamic identification of a potential TF suspicion.

321. In 2016 Liechtenstein conducted its first National Risk Assessment covering period 2013-2015. The NRA was published in 2018. Its second iteration was finalised in July 2020, taking into account data relevant for the period from 2016 to 2018.

322. The 2020 NRA concluded that Liechtenstein faces a moderate TF risk while at the same time determining the threat level of terrorist attacks to be low. The 2020 assessment bases its analysis on a wider set of data and information sources compared to the previous iteration. The 2020 NRA also considered the extent to which the TF threats may exploit the TF vulnerabilities present in Liechtenstein, making it likely for residual risks to manifest themselves through the three internationally recognised TF typologies, i.e., the collection, movement and use of funds for terrorism purposes. The AT finds the overall assessment of TF risks to be reasonable and objective.

323. For purposes of IO.9, an important element with regard to TF risks is the analysis of incoming and outgoing financial flows to/from high-risk countries (see also IO.1). The competent authorities collected relevant data on this matter and have, at their hand, granular information of these inflows/outflows. The AT finds it important that such exercise has been carried out - it assisted the authorities to better understand their exposure to TF threat stemming from high-risk jurisdiction and thus better assess the underlying risks. In absolute terms, these incoming/outgoing funds amount up to 0.9% of the total volume - approximately CHF 2.7 billion for the period reviewed by the 2020 NRA. This figure may be even larger since (as observed in the NRA), transactions to and from abroad are "largely indirect and rarely transferred directly from the country of origin" (though, arguably, this becomes a threat to be considered by the originating or beneficiary country). IO.1 provides further details on this matter, concluding that further analysis of these inflows and outflows would be beneficial given that the one carried out within the framework of 2020 NRA is rather general.

324. During the period under review, seven TF related SARs/STRs were submitted. Overall, the number of SARs/STRs appears low, especially if one takes into account amounts of transactions with high-risk jurisdictions. Consequently, there are some doubts whether the TF related reporting from the entities subject to DAA has been appropriate. In other words, the AT examined whether the fact that seven SARs/STRs were submitted so far indicated that some sectors (primarily banks) might have been insufficiently attentive to certain TF red flags and thus have not been submitting SARs/STRs when there might be reasons to do so. The AT is cognizant that TF threat may arise from jurisdiction's financial products and services being used for TF purposes by individuals or organisations anywhere in the world. One of the principal TF risks for an IFC is to be used as a transit jurisdiction for the movement of funds through the involvement of financial intermediaries. Another example would include the management of foreign funds or businesses linked to terrorist activity outside the country. The AT discussed these issues during the on-site and examined the possibilities of occurrences of these typologies in Liechtenstein. Despite relatively low number of TF related SARs/STRs, the AT observed that persons subject to the DDA have appropriate awareness on TF related reporting (see IO.4) and that the FIU efforts in this direction are appropriate. In addition, the authorities managed to demonstrate that they remain vigilant to these risks and are aware of TF related typologies which may occur in an IFC. However, this does not mean that a thorough assessment on country's vulnerabilities vis-à-vis these challenges should not be an on-going exercise. In the AT's view, it would help the authorities

to better understand if further improvements are needed and address eventual vulnerabilities in the system.

325. Altogether, the AT observed that the competent authorities have appropriate awareness of risks and of potential TF typologies the jurisdiction might be exposed to. Onsite interviews also confirm that they have skills and expertise required to investigate TF (see CI 9.2).

4.2.2. TF identification and investigation

326. Liechtenstein has a sound legal framework to combat TF (see TC Annex). The authorities involved with countering TF are the same as those responsible for fight against ML – the FIU, the National Police, the OPP and investigative judges.

327. With the absence of TF prosecutions and convictions in Liechtenstein, the authorities have not had the opportunity to develop practices in gathering evidence neither to develop jurisprudence on evidence needed to secure conviction for TF. At the same time, the authorities advised, that when TF suspicion arose in the past, they acted diligently.

328. If an international cooperation request on TF is received, the OPP and the National Police are obliged to take all necessary measures to identify TF and to initiate investigations into TF ex officio, in particular on the basis of findings from MLA proceedings or from an international cooperation request received by the National Police. The procedures that the competent authorities follow to identify TF do not differ much from those applied when detecting ML. The authorities advised that any terrorism related suspicion would immediately trigger a parallel financial investigation. This investigation would be considered as top priority and adequate resources would be deployed. The authorities are aware and that a parallel TF investigation in Liechtenstein could be initiated by terrorism offences committed outside the country (see case 2 in the box below).

329. Liechtenstein entered into an Agreement on Operational and Strategic Co-operation with Europol in 2013. The country has also concluded a trilateral treaty on police cooperation with Switzerland and Austria (Liechtenstein Law Gazette 2001, No. 122).

330. Liechtenstein is small country and does not have its own intelligence. For identification of potential TF related cases, Liechtenstein relies on intelligence received from neighbouring countries. The National Police has wide variety of intelligence sources to identify potential TF cases, that include, but are not limited with the following (a) SIENA channel, which is owned by Europol and is aimed to counter terrorism (SIENA CT) and corruption (SIENA ACA); (b) direct encrypted link to German intelligence services (BfV; LfV BW); c) access to Terrorism Screening Centre, a United States database of known or suspected terrorists (d) Liaison Officer Network, that is police-to-police information from FBI, DEA, RCMP, Italy, Spain, Russia, Germany etc. In order to be able to improve the mechanisms to detect TF at an early stage, an instruction/flowchart has been developed by the National Police, to assist the officers to better identify TF. This flowchart/instruction provides all mandatory steps that need to be undertaken in case of a TF suspicion, such as information gathering (from different databases and from foreign counterparts), their analysis and information exchange with competent authorities in country and abroad.

331. Starting from year 2015, up until 2019 the National Police received 13 informal requests for information from foreign counterparts regarding TF. These requests, however, were those

that were addressed to all jurisdictions, and, by virtue of that, reached Liechtenstein. In other words, the information sought had no ties to Liechtenstein. For this reason, the content of these requests was not considered in NRA TF. Authorities advised, that at the moment, statistics would filter different requests and would not take such requests into account for TF related analysis.

332. The OPP has designated two specialised prosecutors for TF proceedings. The OPP and the National Police took measures to develop capacities in identifying, investigating and prosecuting TF, including through regular trainings and exchange of information with partnering institutions in Switzerland, Germany and Austria. In addition, one financial investigator in the National Police was specifically designated to pursue TF cases if and when the need arises.

333. Prosecutors were trained with CRAAFT project, which is an academic research and community-building initiative designed to build stronger, more coordinated CTF capacity across the EU and in its neighbourhood. The project engages with authorities and private entities in order to promote cross-border connectivity and targeted research.

334. With regard to operational work carried out so far, starting from year 2015, the FIU received seven SARs/STRs related to TF. In general, these SARs/STRs had very few links with TF. As a matter of fact, the AT met some of the persons subject to the DDA which submitted TF related SARs/STRs. As an example, one of these SARs/STRs was about the former designated person – subsequent discussions with the FIU confirmed that this person was removed from the sanctions list. With another SAR/STR submitted by a TCSP, funds sent to foreign jurisdiction for charity purposes were under scrutiny, however no TF relation was confirmed.

335. On the other hand, one of the seven SARs/STRs triggered an analytical report which was then disseminated to the OPP. Consequently, an investigation was launched. Details of the case are provided in the box below.

Box 10: TF investigation

An unemployed Turkish national with residence in Liechtenstein, was a subject to an SAR/STR submitted by a bank. The SAR/STR indicate a suspicion that the Turkish national had remitted funds to a non-profit organisation (NPO) in a third country, which hosted an Islamic preacher who spread fundamentalist views. The transfers were suspected to involve two donations of CHF 160 to the NPO. The case was subsequently disseminated to the OPP for further investigation. The suspect had already been under police surveillance due to suspicions that he had been radicalized and had joined a Salafist group. An analysis of the bank account of the suspect revealed that he had remitted funds to the NPO but also to other persons who had connections to the Salafist community in a neighbouring country. Preliminary investigation could not determine that the persons receiving the funds were terrorists or affiliated to a terrorist organization or that the funds were connected to a terrorist act. The behaviour of the suspect on certain social media sites was also scrutinized. However, there was no indication that the suspect had incited terrorism. No TF charges were, therefore, brought against the suspect.

336. Another interesting development, which includes suspicion of TF and ties to Liechtenstein, is provided below.

Box 11- TF suspicion

Further to the terrorist attack in Vienna, an Austrian daily newspaper (November 2020) reported that there were hints of possible ties that the suspects had with charitable and tax-exempt Liechtenstein foundation banked in Liechtenstein. The settlor of the assets on this account is a citizen of Saudi Arabia. Assets in the amount of almost CHF 5.5 million were transferred from an account of a Ltd. domiciled in BVI to the account of the foundation at the Liechtenstein bank. Trustees and authorized signatories on the Foundation's account are a Liechtenstein trust company and two natural persons, residents of the United Kingdom and the United Arab Emirates. During the period November 2019 - April 2020, four transactions from the account of the Liechtenstein foundation, amounting to EUR 133 391 were executed to an Austrian private foundation and to a company which rendered services to this foundation. The payments were intended to serve the purpose stated in the business profile of the foundation, in particular to support charitable institutions in the field of education and culture. Liechtenstein FIU undertook the analysis of the case right after the paper published the article. The analysis confirmed that the recipient of funds (Austrian private foundation and its founder) was associated to the Muslim Brotherhood. Even though the Liechtenstein FIU did not find any evidence of TF, further information exchange was carried out upon request of the Office for the Protection of the Constitution and Counterterrorism (BVT) in Vienna. The FIU thus shared its analytical report with the National Police and requested a contact with the BVT to be established on this matter. Further inquiries have not confirmed that there was any TF suspicion neither that transfers from Liechtenstein foundation had anything to do with TF.

337. Features of these cases confirm the authorities vigilance and pro-active approach in investigating activities with potential links with TF. It is obvious (from case 1) that the authorities properly examine financial profiles of suspects whilst interagency communication and cooperation is ensured. Consequently, actions undertaken confirm that competent authorities are equipped with skills and knowledge to investigate TF.

4.2.3. TF investigation integrated with –and supportive of- national strategies

338. Whilst there is no specific counter-terrorism related strategy developed by the country, AML/CTF Strategy targeting main goals in prevention/suppression of ML/TF has been developed in July 2020. The strategy is based on findings of the 2020 NRA and the specific risks identified therein.

339. Given the fact that Liechtenstein counter-terrorism efforts include close cooperation and reliance on neighbouring countries intelligence networks, the AT considers the approach not to have an independent CT strategy as justified. Furthermore, the AML/CFT Strategy pays specific attention to CTF measures to be applied (or whose application is on-going) allowing the competent authorities to have a clear set of goals in the CFT field.

340. The 2020 Strategy has 4 pillars: 1) Effective implementation of international obligations and standards to combat ML and TF, taking into account the specific risks identified for Liechtenstein; 2) A risk-based focus to increase the effectiveness in combating ML and TF and to improve the risk management by persons subject to the DDA; 3) Ensuring effective ML/TF

prosecution; and 4) Further intensification of national and international cooperation, coordination and exchange of information by the PROTEGE WG.

341. Each of these policy objectives is followed by concrete actions that primarily target the FIU and the National Police requiring them to develop specific instructions for their officers on how to investigate TF.

342. Furthermore, declaration of cooperation was signed between the Court of Justice, the OPP, the National Police, the FMA and the FIU in April 2020. The declaration provides basis for cooperation and information exchange in criminal and judicial proceedings. As a matter of fact, this declaration only formalised the good practice already applied by the competent authorities.

343. Taking also in to account the size and context of the jurisdiction, actions and strategic approach discussed above, the AT is of the view that TF related investigations are integrated with, and used to support, national AML/CFT strategy.

4.2.4. Effectiveness, proportionality and dissuasiveness of sanctions

344. Since there have been no prosecutions/convictions for TF, no conclusion could be made on proportionality and dissuasiveness of sanctions applied. On the other hand, sanctions, as envisaged by the CC for TF offence, appear proportionate and dissuasive.

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

345. Liechtenstein authorities have never been in a position to apply alternative measures in lieu of TF proceedings. As a matter of legislation, two such measures are available in Liechtenstein. These are:

(i) Expulsion of foreigners under Art. 53 (1) Foreigners Act. Foreigners are expelled by order if they have been convicted to an unconditional term of imprisonment of two years or more due to a crime or a misdemeanour or if a preventive measure as defined by Section 3 of the CC has been ordered against them or they have seriously violated or represent a threat to public security and order in Liechtenstein or abroad or represent a threat to internal or external security.

(ii) Revocation of citizenship due to substantial damage of the interests and the reputation of the state pursuant to Art. 21 (1) (b) Civil Rights Act (BüG). Whilst this has not been availed of yet, its *travaux préparatoires* (BuA 2015/66, pages 40 and 41) list some examples when this measure could be applied, including an example when someone joins a terrorist group or commits or participates in terrorist offences.

Overall conclusions on IO.9

346. Even though there have been no prosecutions for TF, the approach taken by LEAs in cases of potential TF occurrences demonstrates that the authorities have adopted a proactive approach in combating TF. The OPP, the judicial authorities and the National Police are well trained and well aware of the TF threat environment IFCs are exposed to, as well as of the fact that the absence of terrorism threat do not exempt them from being vigilant to this phenomenon.

347. The features of one TF investigation carried out so far and the actions undertaken by the competent authorities confirmed that they are equipped with skills and knowledge on how to detect collection, movement and use of funds for TF purposes. Specific TF Strategy has been

developed and is followed by concrete actions by the FIU and the National Police on more practical measures in combating TF. This being said, the authorities need to further their analysis with regard to transactions to/from TF related high risk jurisdictions and to continue monitoring FIs'/DNFBPs' reporting in relation to these transactions.

348. **Liechtenstein is rated as having a substantial level of effectiveness for IO.9.**

4.3. Immediate Outcome 10 (TF preventive measures and financial sanctions)

4.3.1. Implementation of targeted financial sanctions for TF without delay

Legislative and institutional framework

349. Liechtenstein's legal framework aimed at immediate and automatic implementation of TF-related TFS pursuant to respective UNSCRs was introduced in 2017, while a number of legal amendments were further developed, the latest ones being introduced just before the onsite visit. The main legal instrument in place governing implementation of UN TFS into the national framework is the ISA, which is further supplemented with Government Ordinances providing a regulatory framework and general procedures aimed at implementation of the respective UNSCRs (Ordinance of 4 October 2011 on Measures against Persons and Organisations associated with the Taliban, as amended in August 2021 (Taliban Ordinance); and the Ordinance of 4 October 2011 on Measures against Persons and Organisations associated with ISIL (Da'esh) and Al-Qaida, as amended in August 2021 (ISIL/Al-Qaida Ordinance). Based on these legal instruments, the respective UNSCRs (together with their lists) are automatically transposed into the national framework, thus ensuring the implementation of TF-related TFS without delay. Any designation by the UNSC and its committees comes into effect immediately in Liechtenstein.

350. As regards the mechanisms in place for implementation of UNSCR 1373, some shortcomings were in place during the period under review related to the restricted scope of application of the ISA, in particular application of compulsory measures by the Government to enforce sanctions adopted by "the most significant trading partners of the Principality of Liechtenstein". As highlighted by the 4th round evaluation of Liechtenstein, this legislative framework was rather discriminatory and unnecessarily narrowed the application of UNSCR 1373. With legislative changes in 2017, this shortcoming was addressed, and the ISA now applies also to the UNSCR 1373 mutatis mutandis.

351. In June 2020, the Government further issued the Ordinance on Measures against Certain Persons and Organisations to Fight Terrorism (Terrorism Ordinance) which defines the mechanism for identifying targets for designation at the national level and the listing in the annex of the said Ordinance. This was followed in August 2021 by introduction of instructions on the procedure to be followed for requests for: (i) designation on a sanctions list; or (ii) removal from a sanctions list. Based on these, the FIU is the competent authority to identify targets and to make a recommendation to the Government on designations. Based on the ISA, the Government is the decision-making body for national designations and proposing designations to the respective UNSC. Pursuant to the Government's decision, the Office for Foreign Affairs notifies the competent committee of the UNSC of the proposal for designation on the UN list. In addition, the FMA and the Chamber of Lawyers have been vested with supervisory powers related to the implementation of TFS.

352. Due to the very recent nature of these instructions, the AT cannot make firm judgements on the effective use of the mechanisms in place. Nonetheless, meetings with the authorities identified confusion amongst them on their respective roles and responsibilities in the case of a potential designation. On a positive note, the authorities were able to elaborate on the evidential thresholds as well as designation criteria to be applied, mainly referring to those in the respective UNSCRs.

353. Liechtenstein has not yet identified any individuals or entities or proposed any designations under UNSCRs 1267/1989 or 1988, which is consistent with the TF risk profile of the country. Nor have the domestic procedures in relation to UNSCR 1373 been tested in practice due to the absence of such cases. No requests were received from foreign counterparts in this regard. Similarly, there have been no cases of application of TFS by persons subject to the DDA. A regular exchange of views and cooperation between all the relevant authorities is also ensured through the PROTEGE WG.

Communication mechanisms

354. The country has implemented a multi-pronged communication mechanism for informing competent national authorities, the private sector and the public about the sanctions regimes and designations. In particular, the Office for Foreign Affairs, having a coordinating role, circulates new developments and amendments to the UN lists to competent supervisory and enforcement authorities, including Government Legal Services, the FMA and the FIU. In addition, the FIU informs persons subject to the DDA about designations/listings, de-listings, or other modifications of the lists or of the sanctions regimes by a newsletter sent through "goAML". As for the general public, no separate mechanism has been introduced for communication of designations and delisting decisions. At the same time, due to the automatic adoption of UN sanctions lists in Liechtenstein, persons subject to the DDA have an obligation to consult the relevant UNSC websites themselves. Since the introduction of an automatic and thus immediate adoption of UN lists by an amendment to ISA in 2017, the UN lists (i.a. TF related TFS) have no longer been published in the Liechtenstein Law Gazette and have to be accessed from the UN website directly, thus guaranteeing immediate and correct implementation of UNSC sanctions.

355. As regards other information regarding the TFS framework, the Office for Foreign Affairs has published general information regarding UNSCRs, links to national legislation, national authorities, the consolidated UN list, as well as links related to UN de-listing procedures. Additional information can also be found on the FIU's webpage, including the FIU Guideline on implementing the ISA, which provides persons subject to the DDA with information and guidance on: (i) the automatic adoption of UNSC sanctions lists; (ii) obligations to freeze and report; (iii) the mechanism for granting exemptions; (iv) de-listing through the UN Ombudsman for UNSCR 1267/1989; (v) procedure on the request for removal from the UN list to be submitted by the Government upon recommendation of the FIU; and (vi) procedures on delisting from domestic lists.

356. In addition, the FMA has updated FMA Instruction 2018/7 – General and sector-specific interpretation of the DDA to also cover TFS-related obligations for persons subject to the DDA.

357. Obligations of persons subject to the DDA in relation to implementation of TFS are provided under the ISA (immediate freezing and reporting of cases related to TFS to the FIU). Implementation of the TF TFS by the private sector is provided under IO.4, including the

understanding of the private sector representatives, the screening tools they use and the frequency of screening. Persons subject to the DDA demonstrated at least a generally good understanding of TFS-related obligations, while banks and large TCSPs demonstrated advanced practical knowledge in this regard. Smaller DNFBPs explained that they would mostly rely on banks as regards identification and subsequent freezing/reporting. Most would refuse completion of a transaction and would file a report to the FIU in case of a match. However, they were less clear on what would be done when, irrespective of a match, there was also a suspicion of TF. In general, the persons subject to DDA were less clear on their obligations to respect a de-listing or unfreezing action due to lack of guidance in this regard. In addition, due to the very recent introduction (amendments) of TF TFS related instructions and guidance in relation to screening technicalities, most persons subject to the DDA (excluding banks) were not familiar with these documents. Clients are checked against the TFS related lists both at the stage of establishing a business relationship and conducting transactions. Issues noted for some sectors (namely the VASPs and investment funds) in this regard are analysed under IO.4.

358. So far, there have been a few cases of potential true matches (mostly related to EU sanctions). These have been sent to the FIU; however, they have not resulted in asset freezing, being false positives. Only a very limited number of false positive reports have been submitted to the FIU related to UNSCR sanctions lists. In the limited number of cases that included indications of potential TF, the FIU had contacted affected counterparts swiftly and had not received a reply that would substantiate the initial suspicion. At the same time, it should be noted that a number of reports on potential evasion of other sanctions regimes have been filed with the FIU by banks and TCSPs, which demonstrates good awareness of these sectors.

359. As regards measures in place aimed at identifying persons indirectly controlling or owning funds involved in transactions, there are doubts as to the extent to which the majority of persons subject to the DDA are able to comply with this obligation. Whilst the authorities have developed "red flags" related to cases of suspicion of TF, understanding of most persons in this regard is limited to checking existing lists (and persons which might be related to, or act under, the direction or control of listed persons). In addition, as provided under the TC Annex, the Terrorism Ordinance does not provide for the obligation to freeze funds or other assets of persons and entities acting on behalf of, or at the direction of, designated persons or entities.

360. Competent authorities organise PPP meetings on a regular basis, which, inter alia, cover topics related to TF and TFS. Special meetings have also been organised on how the VASP sector in Liechtenstein could affect TF-related risks. Currently no TF related TFS controls are designated to Commercial register, BO register, Ministry of Legal affairs and the STIFA when establishing an entity in Liechtenstein. This issue has been discussed in the framework of the PROTEGE WG and it is still on the agenda.

361. As regards supervisory actions, the FMA and Chamber of Lawyers have been designated as the competent supervisory authorities since January 2020 (see IO.3).

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

Risk assessment

362. The entire common-benefit sector of Liechtenstein has been analysed in a report prepared by STIFA, concluded in May 2020. The analysis was performed using a wide range of

data sources and assistance from involved authorities, including the FIU, FMA, Fiscal Authority, the Court of Justice and the OPP, as well as several interviews with representatives of the NPO sector and survey of the Association of Liechtenstein Charitable Foundations (VLGST).

363. The NPO Risk Report provides an overview of the common-benefit sector in Liechtenstein, including its composition, data on legal forms, nexus to high-risk jurisdictions, critical terms and associations with regard to possible anomalies, and TF indicators. The analysis also includes: (i) FIU evaluation of possible involvement of Liechtenstein common-benefit foundations and establishments and all registered associations in FIU analytical cases for the period from 2016 to 2018; and (ii) information from the OPP and Court of Justice on possible involvement of Liechtenstein NPOs in domestic criminal proceedings and MLA between 2016 and 2018. The analysis reveals that the preferred legal forms for common-benefit organisations in Liechtenstein are primarily foundations and associations, while establishments are also considered a relevant legal form. As of 31 December 2019, Liechtenstein has identified 1 436 common-benefit organisations that fall under the FATF definition. The report provides for possible TF misuse typologies and defines the following risk criteria, the presence of any of which an NPO would be classified as high-risk: (i) nexus of contributors and governing bodies to high-risk countries; (ii) low integrity and reputation of partner organisations; (iii) purpose linked to high-risk countries or terrorist organisations; (iv) geographic exposure due to direct funding of activities in high-risk countries; (v) especially high assets; (vi) involvement in FIU analyses, criminal investigations, proceedings or MLA proceedings of LEAs; or (vii) negative media profile.

364. Based on collected data and analysis it was concluded that, out of a total of 1 384 common-benefit foundations and establishments falling under the FATF definition of NPO, 44[18] present a high-risk. Out of a total of 52 associations falling under the FATF definition of NPO, eight were identified as high-risk.

365. At the same time, the analysis for foundations and establishments concluded that: (i) donors (founders) are commonly from Liechtenstein and other European countries; (ii) TF risks associated with cross-border transactions are mitigated to a large extent by the use of partner organisations with a high level of professionalism and reputation, predominantly domiciled in Europe; and (iii) common-benefit foundations and establishments are subject to a wide range of risk-mitigating measures, including supervision and appointment of a qualified member (as further described below). Overall, the residual sectoral TF risk of common-benefit foundations and establishments classified as NPOs was therefore assessed as medium-low. As for associations, the authorities concluded that funding comes from members or through smaller fundraising events held in Liechtenstein. Therefore, funds usually come from Liechtenstein residents and, due to the Liechtenstein nexus, are regularly and mainly distributed in Liechtenstein. Associations do not manage large amounts and hardly have any international presence. On this basis, the risk for common-benefit associations classified as NPOs was assessed to be low.

366. It should also be noted that, based on these outcomes, the authorities have already introduced some mitigating measures, while others are planned.

[18] One foundation was identified as a high-risk NPO at a later stage, i.e. after the NPO Risk Report was adopted in May 2020, and therefore, is not included in the 44 high-risk NPOs. In addition, one foundation that was identified as a high-risk NPO was deleted in the meantime.

Risk-based monitoring and supervision

367. Monitoring/supervision of the NPO sector is conducted by several authorities, including STIFA and the Fiscal Authority, as well as the FMA as regards the supervision (as TCSPs) of qualified members of the governing body of NPOs.

368. Common-benefit foundations and establishments are required to register by being entered into the Commercial Register and thus acquiring legal personality. Associations are only obliged to be entered into the register if they conduct business in a commercial manner for their purpose or are subject to an audit. Otherwise, registration is voluntary. In practice a large proportion of associations are registered in the Commercial Register, including the ones identified as falling under the FATF definition of NPOs. All legal persons, including those applying for tax exemption, are also registered with the Fiscal Authority. Regarding tax exempt NPOs, the Fiscal Authority reviews the annual external audit report, audited annual financial statements, or a list of assets and any statement of appropriation of assets to evaluate whether those entities comply with the requirements for granting tax exemptions.

369. Another important risk-mitigating measure is the requirement for a qualified member to be appointed to the governing body (Persons and Companies Act, Art. 180a) for all legal persons. As a TCSP, the qualified member must apply DDA/DDO obligations to the NPO – its customer. This includes identification of the BO, monitoring and filing reports with the FIU. Supervision of the activities of qualified members is conducted by the FMA directly or through commissioned auditors (see IO.3 and IO.5 where limitations in supervision are identified). Both the FMA and commissioned auditors are required to submit a report to the FIU where ML/TF arises. Between 2016 and 2020, the FMA has not filed any such reports.

370. While there is also a requirement to appoint a qualified member to the governing body of associations, so far this has not been applied in practice. Thus, the formal monitoring/ supervision over associations is conducted by the Fiscal Authority.

371. As regards STIFA, it *ex officio* ensures that the assets of foundations and establishments are managed and used in accordance with their statutory purpose. This is done through annual inspections conducted by court-appointed auditors and through STIFA on the basis of a three-year inspection cycle, if the common-benefit foundation is exempt from the obligation to appoint an auditor as the foundation only manages minor-value assets or the exemption seems expedient for other reasons. As in the case of the FMA, STIFA is also required to submit an SAR/STR to the FIU, which has been the case in five instances related to ML suspicion between 2016 and 2020. No cases related to TF suspicion have been identified so far.

372. The supervisory activities conducted by the competent authorities over foundations and establishments cover the whole range of activities provided under INR.8 as regards monitoring/supervision exercised. These activities were applied to all common-benefit foundations and establishments in an undifferentiated manner until the adoption of the NPO Risk Report, so that a risk-based approach, including a focus on TF aspects, was not implemented (in relation to the NPOs identified as high-risk NPOs). However, there has been a strong commitment by the authorities to enhancing their efforts in this regard. Based on the results of the NPO Risk Report, the authorities have developed an activity plan on conducting bilateral supervision meetings with high-risk NPOs. These meetings raise awareness, rather than inspect. The first supervisory meetings started in March 2021 and were due to be completed by the end of 2021.

By the end of August 2021, the majority of planned meetings had already been carried out (i.e., supervisory meetings have been held with 43 out of 52 NPOs identified as "high-risk" NPOs). The presentation, which forms the basis of the supervisory meetings, has been shared with the AT. Moreover, the names of the identified high-risk NPOs have been communicated to the FMA at the beginning of April 2021 in order to subject the TCSPs administering these NPOs to more intensive FMA oversight. These are positive steps, while further action would also be expected to be taken for associations, to the extent that this does not disrupt their legitimate activities.

Outreach and awareness

373. Common-benefit foundations and establishments have been provided with several training sessions. STIFA published a factsheet for NPOs on TF risks (in German and English) in March 2013, which was last updated in November 2020 on the basis of the findings of the NPO Risk Report. This factsheet was prepared jointly with the FMA, FIU and the Fiscal Authority. In addition, awareness raising initiatives on developments in the field are also conducted by the VLGST through sharing information on its website, organising training and issuing publications. The FIU and STIFA are regular speakers at the annual meeting with authorities of the VLGST. Apart from the STIFA factsheet, no similar initiatives have been undertaken for associations during the period under review.

374. As regards the awareness of NPOs met, foundations and establishments demonstrated good knowledge on their TF TFS related obligations and sector specific risks. This was also demonstrated by the TCSPs acting as qualified members of the governing bodies to the NPOs. This, however, cannot be confirmed for the associations sector. The association met onsite did not have any knowledge in this field. Guidance and outreach, together with introduction of mitigating measures, is thus required to ensure that associations are not misused for TF purposes.

4.3.3. Deprivation of TF assets and instrumentalities

375. Liechtenstein has in place to a large extent a comprehensive legal framework that establishes appropriate mechanisms for the freezing/confiscation of assets of persons involved in TFS (see also R.6 in the TC Annex). Although no assets have been frozen under the respective sanctions regimes set out in UNSCRs 1267/1989, 1988 or 1373, the competent authorities have demonstrated their ability to take action under other UNSCR sanctions regimes to freeze assets, funds and ensure prohibition of access to frozen funds.

Box 12: Case study related to other sanctions regime

Case 1. The case dealt with a country X entity listed under the EU sanctions regime. The foreign entity holds a bank account in Liechtenstein. This was reported to the ISA authority (the FIU) and the FIU's analysis found indications that the former ultimate BO had been replaced a few days before the said entity had been listed under the EU sanctions regime. The Office for Foreign Affairs was then tasked with contacting their Country X counterparts in order to locate the appropriate counterpart in charge of TFS. As soon as this was done and confirmed by the country X authorities, the FIU contacted its counterpart in Country X and provided full details of the case. The response from Country X authorities is still pending and thus there have been no updates concerning this case.

Case 2. A TCSP with a business relationship with a Liechtenstein charitable foundation, was alerted by a planned outgoing disbursement of funds. Due to the nature of the foundation's purpose and activities (finance of Islamic educational programmes in Europe, finance of travel programmes for students etc.) the business relationship was put into a high-risk category. Accordingly, every donation was checked thoroughly before its disbursement. In this case, a transaction was planned to be made in relation to an academic employee of a world-renowned educational institution abroad. This individual was subject of an OSINT research conducted by the foundation, and it was revealed that this person might have potentially been a member of a HAMAS delegation visiting the Malaysian ruling party some ten years ago. The FIU then contacted its counterparts in the country where the educational institution is domiciled and received a negative reply. Hence, this case was no longer viewed as a TF case and archived for further analysis in case new information is received in the future.

376. Liechtenstein has not conducted any terrorism or TF-related prosecutions or convictions which would have resulted in depriving subjects or organisations of assets and instrumentalities related to TF activities; there has also been no case of a (non-conviction based) confiscation of such assets. No other measures to deprive terrorists of their assets have been applied.

4.3.4. Consistency of measures with overall TF risk profile

377. The TF NRA has concluded that there is a medium risk of Liechtenstein being misused for TF purposes based on medium threat level, a medium sector-specific risk and a medium vulnerability level. While financing activities involving the collection or use of funds in Liechtenstein for terrorism purposes are determined to be low, the risks associated with the movement of funds through Liechtenstein are considered to be medium. Given the relative importance of funds movement activities in the Liechtenstein context, the risk rating assigned is medium.

378. The measures undertaken by the competent authorities, as described under this chapter, appear to be consistent with the jurisdiction's overall TF risk profile. The relevant NPO supervisory authorities did not reveal any indication of abuse of the NPO sector for TF purposes. There has been one SAR/STR filed with regard to a common-benefit foundation, however, no further actions were required based on the FIU analysis.

379. As for associations which fall under the FATF's NPO definition, the authorities have already taken certain measures in relation to these. In particular, bilateral meetings have been organised with the associations identified as high-risk NPOs. In addition, the authorities have included an action in the NPO Risk Report action plan aimed at considering the mandatory introduction of qualified members for governing bodies of those associations falling under the FATF definition of NPO. Nonetheless, the actions taken by the authorities so far do not yet constitute a risk-based monitoring/ supervision in relation to associations.

Overall conclusions on IO.10

380. Liechtenstein's national legal framework ensures immediate implementation of TFS. Effective communication mechanisms have been introduced. Due to very recent nature of some of the legislative amendments (mainly listing/delisting procedures) and guidance/instruction provided to the private sector, the latter were not fully enforceable at the time of the onsite. Some small and medium-sized persons subject to the DDA were not able to explain exactly what new

requirements had been imposed by a new TFS guideline issued more recently by the FIU. No TF TFS related assets have been frozen or confiscated so far.

381. The country has identified the NPOs which fall under the FATF definition of NPO (and could be at risk of TF misuse) through a comprehensive risk assessment, however not all NPOs (in particular, associations) are yet subject to full risk-based monitoring or supervision. Authorities have provided outreach to foundations and establishments, which demonstrated good knowledge in this regard. This was not confirmed for the association met onsite.

382. **Liechtenstein is rated as having a moderate level of effectiveness for IO.10.**

4.4. Immediate Outcome 11 (PF financial sanctions)

Contextual factors

383. Liechtenstein is an IFC specialised in providing banking, TCSP and insurance services predominantly to foreign customers. Liechtenstein is neither a dual use goods/ weapons manufacturing jurisdiction nor has a market of proliferation goods. None of the banks offers trade financing. It has limited trade relations with Iran and no trade relations with North Korea.

384. Under the 1923 Customs treaty between Liechtenstein and Switzerland, the country became an integral part of the Swiss Customs Territory. At that, the authorisation procedures and enforcement (controls and sanctions of infringements) lies exclusively within the competence of the Swiss authorities - SECO and Swiss Customs respectively. SECO is the designated import and export authority for both Switzerland and Liechtenstein. This includes control of exports of dual-use goods, specific military goods, war materials and goods subject to the Swiss catch-all clause.

385. During the period under review, there were two banks in Liechtenstein having indirect shareholders with family ties to Iran. One of these two banks had focused its business model on Iran and was prohibited by the competent authority from doing so in 2018. The second institution oriented its business model towards Middle East with a focus on Iran. A number of supervisory measures were conducted in relation to this second bank. The AT discussed the related issues with the authorities during the onsite, and it was told that the ownership structure and the business model of the bank was undergoing a reform, in other words the shares of the Iranian shareholder were about to be sold. The AT also met the representatives of this bank, further to which it reached a conclusion that proper measures have been implemented in relation to the prevention of PF TFS evasion (discussed below in more details).

4.4.1. Implementation of targeted financial sanctions related to proliferation financing without delay

386. Liechtenstein implements PF related TFS without delay based on the ISA, Government ordinances on Iran (Ordinance of 19 January 2016 on Measures against the Islamic Republic of Iran, as amended) and North Korea (Ordinance of 24 May 2016 on Measures against the Democratic People's Republic of Korea, as amended). The legal basis for the application of TFS under UNSCRs 1718 and 1737 and their successor resolutions is the same as for TFS related to terrorism and TF. Implementation of TFS related to PF follows the same processes and procedures as with TF sanctions (see IO.10). In practice, no distinction is made between TF and PF related TFS.

387. As in case of TF TFS, the implementation of PF TFS without delay is guaranteed by the automatic adoption of UNSC sanctions lists by the ISA and respective ordinances. Thus, any designation by the UNSC comes into effect immediately in Liechtenstein, i.e., FIs and other persons subject to the DDA are required to freeze assets of any person or entity as soon their name is included in the UN lists. Amendments to the sanctions lists and new designations are communicated to persons subject to the DDA in the same manner as in case of TF TFS.

388. As regards national cooperation mechanisms, the PROTEGE, together with the issues related to ML/TF also serves as a platform for exchange of information, views, and expertise on implementation of UNSCRs on PF TFS. Exchange of information between all relevant authorities within the working group is conducted on a regular basis and includes, *inter alia*, informal exchange of data regarding potential PF evasion and cases related to it. Sub-groups are established under the lead of the OPP in order to deal with specific cases. In addition, a bimonthly exchange between representatives of the FIU, OPP, FMA, STIFA and the Fiscal Authority takes place in order to discuss potential cases, supervisory cases as well as measures/sanctions applied thereof. The FIU and the Office for Foreign Affairs exchange information with SECO on a regular basis. Information from these authorities on activities in their area of competence which are relevant to PF are shared within the PROTEGE under the agenda item "Tour de Table". Whilst the AT finds this initiative useful, nonetheless, taking into account the fact that controls on export and import are solely exercised by the SECO, the country might benefit from further enhancement of cooperation with SECO, including through the involvement of SECO expertise in the PROTEGE to better safeguard the system from being misused for PF or related sanctions evasion.

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

389. During the period under review no assets have been frozen pursuant to UNSCRs related to PF TFS. There hasn't been any case reported or investigated by competent authorities either.

390. At the same time the AT was presented with several cases related to other sanctions evasion, involving links to Iran, which demonstrated the ability of persons subject to the DDA to take action in case of a potential PF related case. In all these cases, persons subject to the DDA approached the FIU based on a hit against internal compliance databases. In particular, from 2018-2020 the FIU has been consulted regarding potential breaches of sanctions related to TF/PF (Iran) in two cases. In two other Iran related cases, persons subject to the DDA (one bank and one TCSP) were unsure how to proceed after a potential breach of US Office of Foreign Assets Control (OFAC) sanctions. In all these cases the amounts have been immediately frozen and remained frozen at the time of the onsite.

391. In one case, following a designation under the EU sanctions regime not related to PF, several ISA reports were submitted by persons subject to the DDA on the assets held by them, which were related to the designated person. In this case the assets were duly frozen, while the foreign counterpart, where investigation concerning a designated person was underway, was advised to get back to the Liechtenstein authorities with a formal MLA request.

392. Although these cases were not related to the evasion of UN PF-related TFS, they show the ability of the FIU as an ISA authority to identify and detect sanctions evasion schemes, including through international cooperation. The cases further demonstrate the general vigilance of persons subject to the DDA in complying with their obligations in relation to sanctions evasion.

At the same time, a number of shortcomings were identified on their PF TFS understanding and screening procedures, as well as the supervision in place, presented below. At that, the AT cannot fully confirm the effectiveness of the measures aimed at identifying the assets and funds held by designated persons/entities.

4.4.2. FIs, DNFBPs and VASPs' understanding of and compliance with PF TFS obligations

393. As in case of TF-related TFS, persons subject to the DDA mainly rely on their IT screening tools and name-based screening for the purpose of identifying potential PF cases. Persons subject to the DDA met onsite, in the majority of cases, did not differentiate between TF and PF-related TFS. The level of understanding of their obligations differs among the sectors, with banks and TCSPs having a better level of knowledge in this regard. Most persons subject to the DDA were clear on their respective obligations related to identification, freezing, and reporting of TFS related cases, while the smaller DNFBPs would mostly rely on banks as regards identification and subsequent freezing/ reporting. Most met onsite would refuse completion of transaction and would file a report to the FIU in case of a match. Nonetheless, those met onsite were not always clear on possible typologies of sanctions evasion. In addition, most of the persons subject to DDA were less clear on their obligations to respect a de-listing or unfreezing action due to lack of guidance in this regard.

394. Most of persons subject to the DDA (except for smaller DNFBPs with less clientele) use robust software tools (this mainly being World Check) to screen their existing and potential clients against the UN designations and to detect funds owned thereof. The systems in place provide for the possibility to automatically screen the name of the customer through the list provided not only by the UN, but also EU, OFAC and the lists published by Swiss authorities. Whenever the FIs and some of the TCSPs come across a possible match with sanctions lists, an investigation is opened to confirm whether the match is a true or a false positive one.

395. Clients are checked against the TFS related lists both at the stage of establishing a business relationship and in any case of occasional transaction. Regular checks of the client base are conducted during the business relationship, while the systems in place also review the client base automatically when a new entry is made to the database. Banks screen their database at least weekly (some also claimed daily automatic screening). In other sectors, screening is performed immediately after notification of list changes by the FIU and at monthly to quarterly intervals. Smaller DNFBPs screen their potential and existing clients against the UN lists manually upon receiving information from the FIU. As for the casinos, all of them use commercial databases, which cover UN designations. Their clients are checked at the entrance and in case of a match would be refused to enter the premises, whereas this would also follow asset freezing for the customers having accounts with the casinos.

396. The practices and shortcomings identified under IOs 4 and 10 related to the screening of clients by the VASPs and investment funds are equally applicable in case of PF TFS. As in case of TF TFS, there was a confusion among persons subject to the DDA which reporting regime should be followed in case of a suspicion of potential PF related sanctions evasion, when this is not connected to a true match. As regards the authorizations for import/export of dual use goods, this is directly made available for the banks which use SECO lists for the purpose of checking the status of authorizations. Such access has not been granted to other persons subject to the DDA.

397. In general, as confirmed by the authorities, persons subject to the DDA do comply and mostly understand their obligations regarding TFS well in the context of "direct control", meaning a clear hit (including false positives) against internal and/or commercially available sanctions screening tools. However, as mentioned above, indirect control is more difficult concept for them and thus more difficult to be detected for almost all FIs, VASPs and DNFBPs. This has also been noted by the FIU through various meetings held with the private sector.

398. As regards the awareness raising initiatives and guidance provided to the private sector, these are identical to those carried out/prepared in respect of TF TFS. No PF TFS specific guidance has been issued so far by the authorities. At the same time the AT commends the initiatives held by the FIU on awareness raising in relation to potential PF through trade finance. The typologies presented involve seemingly legitimate companies incorporated in higher-risk IFCs which trade in goods that can also be used as weapon manufacturing materials or dual-use goods, such as fertilizers and technical components of vehicles as an example but can also include very specific miniscule components like bolts and screws.

4.4.3. Competent authorities ensuring and monitoring compliance

399. The competent authorities ensuring compliance and monitoring on compliance with the TF related TFS are the FIU (acting as the ISA authority), the FMA and the Chamber of Lawyers. The FIU is responsible for implementing PF related TFS, as well as monitoring of their implementation by other stakeholders, persons subject to the DDA and the general public.

400. No PF TFS related supervision has been in place throughout most of the period under review. Since January 30, 2020, the DDA supervisory authorities, namely the FMA and the Chamber of Lawyers, have been entrusted with the authority to monitor compliance with the special obligations of persons subject to the DDA (Art. 2c ISA) by means of inspections and off-site supervision. The FMA has developed a thematic inspection program in relation to TFS compliance, but has not included PF-related topics e.g., trade finance.

401. Since then, the FMA has conducted some onsite inspections, including in relation to 6 TCSPs, 4 banks, 1 insurance company and 1 insurance broker, 2 asset management companies and 2 casinos. With these checks carried out, the supervisory authority was able to get a first general impression of TFS compliance in the individual sectors. At the same time, no serious infringements were identified. These inspections were carried out either by the FMA directly, or through commissioned auditors. In addition, the authorities informed that an annual TFS related questionnaire is now in the process of development.

402. The FMA has included some explanations in the FMA Guidance 2018/7 regarding special obligations under Art. 2c ISG, which apply to persons subject to the DDA. Nonetheless, this guidance mainly covers list-based screening obligations, while no red flags/typologies are provided specifically on PF. Awareness raising training was delivered in September 2020 to supervisors/auditors on International Sanctions. No such initiative has been organised for persons subject to the DDA.

403. As regards the Chamber of Lawyers, those exercise supervisory powers in relation to lawyers under the DDO. The supervision is conducted through checks of mainly policies and procedures, while further improvements would be needed in this regard. No targeted PF TFS supervision has been conducted so far.

404. No sanctions or penalties have been imposed for failure to comply with PF-related TFS obligations by any of the authorities during the period under review. Nonetheless, taking into account that the TFS supervision has only recently been introduced, the AT cannot confirm the extent to which the absence of sanctions is justified, and neither can assess the extent to which effective, proportionate, and dissuasive sanctions would be in practice applied by the supervisory authorities.

405. As mentioned earlier, the FIU acts as the ISA authority. At that, it does not act as an administrative type FIU, but has the power to act as a semi-investigative body. The FIU is given the power in the ISA to collect any documents and information it deems necessary to analyse and disseminate it to law enforcement. A case example of the FIU executing its powers as an ISA authority is presented below.

Case Study- Potential circumvention of Iran Sanctions

The FIU learned from a newspaper article in early 2020 that a large quantity of gold had been exported from Liechtenstein overseas. This fact and the additional information that the top two recipients were country x and Iran caught the eye of the FIU. As Liechtenstein has formed a customs union with Switzerland and therefore does not have a domestic border authority, the FIU asked the Liechtenstein Embassy in Bern to approach the Swiss Main Customs Directorate to receive more detailed and segregated documents and information on exporters and their customers. This information was provided by the Swiss counterpart authority in due course. It revealed that apart from certain firms operating in specific industries (i.e., coating, dental, automotive, construction etc.) that regularly import and export precious metals, one foundation and one European legal entity had been by far the largest recipients of gold exports. The mentioned foundation had bought 3.5t of Gold worth CHF 166 million with destination country x, while the European legal entity bought about half that amount with destination to Iran. The FIU analysis further revealed that the European entity was closely connected to the Iranian Bank A, which is not sanctioned under EU or Liechtenstein sanctions regimes. Previously, the above-mentioned facts and circumstances had been unknown to the FIU and had not been reported to it. The FIU, acting as ISA implementing authority in this case, contacted the DPMS responsible for the export of said metals and requested a variety of documentation and information. Shortly afterwards, the FIU met with the dealer`s attorney and the following facts were revealed:

- it was confirmed that the European legal entity was the ordering party, and that Iranian Bank A in Iran was the recipient per official documentation (i.e., cargo shipment documentation).

- it was revealed that Iranian nationals visited Liechtenstein prior to the conclusion of the purchase to see the premises and go through details of the transport etc.

- it was revealed that Iranian Bank A had transferred the agreed amount to an account held with a 3rd country bank, and that the Liechtenstein DPMS had previously opened an account with the same third country bank to receive the Iranian funds.

Once the gold had left Zurich Airport, there is no confirmation that it was directly transported to Iran or whether stopovers were made. The question still remains whether the gold fell into the hands of sanctioned natural or legal persons in Iran once it was transported there.

406. The ISA is not limited to reporting/regulated entities but is extended to any person. While collecting information on-site FIU staff can request the National Police to accompany them and

file a request with the OPP and the investigative judge for natural persons to be summoned for interviews. In addition, it is empowered to conduct ISA evaluations in the form of bilateral meetings and discussions with persons subject to the DDA. Authorities advised that, on average, the FIU has held 5-10 ISA evaluations annually, predominantly with banks and TCSPs. In addition, sanctions-related phone calls, not detailing the exact circumstances of a potential case, occur at least once a week, mainly between the FIU and attorneys representing unnamed clients/persons subject to the DDA. Overall, the AT is of the view that the FIU is entrusted with and in practice applies a broad range of powers aimed at implementation of TFS and monitoring of implementation by persons subject to the DDA, which has also been confirmed through the case examples shared with the AT during the onsite.

Overall conclusions on IO.11

407. As in case of TF TFS the country has introduced a comprehensive legal framework aimed at implementation of PF TFS without delay. Due to the recent nature of part of legislative amendments the effectiveness of the overall system, cannot be fully assessed. Trainings have been delivered by the FIU to persons subject to the DDA on the topic of sanctions evasion, including through trade finance.

408. Persons subject to the DDA had generally good understanding of PF TFS, while many of them still do not differentiate between TF and PF TFS. Issues were also noted in relation to their ability of identifying indirect control or ownership. Smaller FIs, VASPs and DNFBPs (apart from TCSPs) lacked guidance on their respective obligations in relation to reporting under different regimes, as well as red flags/ typologies on potential sanctions evasion without a hit in the system. Issues related to the screening processes identified in relation to VASPs and investment funds (see IO.4) similarly apply, which comply with this requirement only to some extent.

409. TFS suspicions have been communicated to the FIU under other sanctions, however not resulting in a formal reporting. No PF TFS related assets have been frozen so far.

410. Supervision of PF TFS has only been introduced since 2020. The FMA has conducted several inspections starting from 2020, but so far, no breaches have been identified. No targeted TFS related inspections have been carried out so far by the Chamber of Lawyers. Overall, no sanctions have been applied, however the extent to which this is justified cannot be confirmed.

411. **Liechtenstein is rated as having a moderate level of effectiveness for IO.11.**

5. PREVENTIVE MEASURES

5.1. Key Findings and Recommended Actions

Key Findings

Immediate Outcome 4

a) Understanding of ML/TF risks and obligations is now generally good among covered FIs, DNFPBs and VASPs. This was not the case for all the period under review. Banks demonstrated the most sophisticated level of understanding of ML/TF risks (linked to private banking and wealth management and use of cash) and obligations and were able to articulate their own sectoral and business wide risks. Among non-bank FIs, the understanding of obligations was also good, but there was less understanding of how their business could be misused for ML/TF purposes. Amongst DNFBPs, TCSPs and casinos have the best understanding of risks and obligations (especially large TCSPs). The understanding of large VASPs was at the same level as large TCSPs, while the understanding of risks and obligations of other VASPs is less developed. Banks and large TCSPs demonstrated the most advanced knowledge of TFS related obligations.

b) In general, mitigating measures are now effectively applied and are commensurate with risk. This was not the case for all the period under review, e.g., less attention was given to establishing and corroborating SoW and SoF and to the possible illicit uses of "shell" companies. Banks and large TCSPs have implemented sophisticated measures to mitigate ML/TF risks. In particular, there are risk-based measures in place to deal with high-net-worth individuals, use of cash, tax substance, and "complex" structures. TCSPs are also actively involved in the day-to-day administration of legal persons and legal arrangements, which involves close oversight of activities and transactions. Across all sectors, there is uneven understanding and implementation of measures to deal with "complex" structures. Measures in place in other sectors are less robust but still satisfactory.

c) Investment funds widely apply an exemption that means that they are not required to identify and verify the identity of underlying investors in units held by subscribing intermediaries (banks) in non-private investment funds - where risk is assessed as low. However, those using this exemption often do not have sufficient information (including information on internal control systems of subscribing banks) available to adequately assess ML/TF risks. Accordingly, it is not clear that the exemption is applied in accordance with requirements. The effect of the exemption also cascades to other sectors where the investment funds are customers.

d) In general, CDD and record-keeping obligations are being diligently applied. Risk-based measures are in place that include all the general elements of CDD (including identification of the BO), on-going monitoring and record-keeping. However, weaknesses have been identified during the period under review in respect of information held on SoF and SoW, with improvements noted following the strengthening of supervisory measures in 2019, and with

customer profiling in the VASP sector. Business relationships are refused if it is not possible to conduct CDD and the submission of a SAR/STR is considered (though with little reporting in practice). Record-keeping measures have been applied in line with R.11 by all sectors.

e) Generally, enhanced measures have been applied appropriately for: (i) PEPs; (ii) new technologies; (iii) wire transfers; (iv) TFS relating to TF; and (v) higher-risk countries identified by the FATF. Whilst FIs do not offer correspondent relationships, except for foreign subsidiaries, VASPs have relationships with similar characteristics. The effectiveness of measures regarding wire transfers and TFS have been hindered in the VASP sector, as the travel rule is not fully implemented in practice.

f) During much of the period under review, reporting obligations were met only to a limited extent. Whilst there has been a significant increase in reporting since 2019, there has been less reporting than expected in respect of tax offences. Many persons subject to the DDA have never filed a SAR/STR, e.g., some TCSPs and asset managers, and some banks and TCSPs have been reported by the FMA to the OPP for failing to make reports. Late reporting has also been observed in the TCSP and VASP sectors. NRA II has also identified factors that have depressed reporting levels for banks and TCSPs. Some smaller non-bank FIs and DNFBPs were unable to elaborate on typologies that could give rise to a SAR/STR. Internal policies/procedures and training are in place to prevent tipping-off but a recent court case highlights a need for additional guidance to be provided by the authorities.

g) FIs, DNFBPs and VASPs have generally good controls and procedures. AML/CFT compliance functions are properly structured and resourced and involve regular internal audits and training programmes.

h) There remain some minor gaps in the scope of application of AML/CFT requirements.

Recommended Actions

Immediate Outcome 4

a) To support reporting obligations, the FIU should provide more granular sectoral guidance (especially for non-bank FIs and DNFPBs) and training on sector specific ML/TF methods trends and typologies, including major risks identified in the NRA. The FMA should contribute its supervisory findings in this regard. Reporting levels across sectors should continue to be monitored by the FMA and anomalies (e.g., late reporting, reluctance to file SAR/STR due to inability to conduct CDD) identified and resolved. Authorities should also take measures to review (and, as necessary, improve) the reporting process in those persons subject to the DDA (including TCSPs) that have never filed a SAR/STR.

b) The FMA should continue its efforts to strengthen ML/TF risk understanding across non-bank FIs, DNFBPs (other than casinos and large TCSPs) and small VASPs such that business specific risks are understood and articulated. BRA and CRA processes should be further strengthened in these sectors.

c) The FMA should continue its efforts to strengthen customer profiling in the VASP sector and to improve documentary evidence held to corroborate SoF and SoW in the TCSP sector, in particular for legacy customers where remediation continues.

d) The FMA should ensure that measures are applied consistently by investment funds in line with the DDA to be sure that the exemption available for investors in non-private investment funds is used only where risks are low.

e) The FMA should provide further guidance on "complex structures" in support of a more even application of EDD measures.

f) As the global implementation of the travel rule progresses, the authorities should take measures to confirm that the "travel rule" is applied in practice by all relevant VASPs.

g) The authorities should provide guidance on what constitutes tipping off in cases where FIs and TCSPs share information in respect of potential clients.

h) The authorities should extend the scope of the DDA to address minor gaps in the scope of application of AML/CFT requirements.

412. The relevant IO considered and assessed in this chapter is IO.4. The Recommendations relevant for the assessment of effectiveness under this section are R.9-23, and elements of R.1, 6, 15 and 29.

5.2. Immediate Outcome 4 (Preventive Measures)

413. As an IFC, Liechtenstein is strongly oriented to providing services to wealthy individuals who are resident abroad. The focus of FIs is mainly on wealth management. The most important of the FIs are the banks, which, including their foreign group companies, managed around CHF 365.4 billion in assets as of 31 December 2020 and are mainly active in private banking and wealth management. Amongst DNFPBs, the TCSP sector is the largest sector, as the establishment and administration of Liechtenstein legal persons and legal arrangements, as well as of foreign legal persons, is one of the core services offered in Liechtenstein. The value of bankable assets administered by TCSPs accounts for roughly 20% of assets held by banks based in Liechtenstein. No estimate is available for the value of non-bankable assets held in legal persons and legal arrangements. The VASP sector holds assets with a value of around CHF 150 million and is dominated by one large provider.

414. Section 1.4.3 of Chapter 1 provides information on the relative importance of each sector. Based on materiality and risk of services and products offered by the banks and assets held by them, the banking sector is weighted as the most important. Amongst DNFPBs, the TCSP sector is the largest sector and weighted as most important. Fund management/asset management, insurance undertakings and VASPs are weighted as highly important. All other sectors are weighted as a moderately or less important.

415. The following activities which are covered by the FATF definition of FI are not subject to preventive measures: (i) lending (own funds only); (ii) financial leasing; and (iii) issuing and managing paper-based means of payment. These gaps are considered only minor in light of the country's focus on wealth management. Provisions in respect of legal and accountancy services do not apply to preparing for or carrying out transactions for clients with respect to the creation,

operation or management of legal persons or arrangements. However, in practice, these activities are provided by TCSPs. As explained under Chapter 1, lawyers providing services related to forming and managing legal persons and legal arrangements do so under the umbrella of a TCSP engaged in establishing legal persons and trusts. TCSPs are also licensed to provide tax advice, and so the extent to which external accountants may be needed to provide input with respect to the creation, operation or management of legal persons or arrangements will be limited. Accordingly, gaps in respect of legal and accountancy services are also considered only minor. There is no general regulation of transfers of VAs which is called for by the FATF Recommendations. Instead, persons that provide such a service are covered as part of regulated VASP activities.

416. Liechtenstein AML/CFT requirements do not apply in relation to business conducted remotely in Liechtenstein by EEA FIs or Swiss insurance undertaking and intermediaries operating within the scope of freedom to provide services. Under EEA arrangements and bilateral agreement with the Swiss, home country requirements apply to such business conducted in Liechtenstein.

417. Whilst the majority of customers are non-resident, there is usually direct physical contact between relationship managers and their customer.

418. The AT's findings on IO.4 are based on interviews with a range of private sector representatives, supervisory findings and enforcement actions, and information from the Liechtenstein authorities (including the NRA).

5.2.1. Understanding of ML/TF risks and AML/CFT obligations

419. Understanding of ML/TF risks and AML/CFT obligations is now generally good, though it varies according to the sector and size of the person subject to the DDA.

Banks

420. In general, banks demonstrated a good understanding of the ML/FT risks to which they are exposed. They can articulate their own sectoral and business-wide risks and appropriately describe different ML/TF risks. Banks prepare business risk assessments (BRA) taking account of the NRA, FMA guidelines and customer risk assessments. Most of the banks demonstrated that their assessments are updated regularly (in most cases annually) or when other internal or external factors trigger an earlier need, e.g., change of business model, expansion into a new market, or launch of new products and services. The BRA methodologies followed involve: (i) identification of inherent risk; (ii) determination of mitigating measures; and (iii) assessment of residual risk. For branches and subsidiaries, assessments generally take into account the group-wide assessment of ML/TF risks. Methodologies used by banks, in general, are considered to be fair and sound.

421. All banks have developed risk appetite statements, deviation from which is allowed only based on substantiated justification and with prior approval from top level management or the parent company (in case of group). In the case of deviation, EDD and monitoring measures are applied. The majority of banks met during the onsite visit mentioned that they do not accept customers that do not align with their wealth management business model, e.g., customers in the defence sector or which trade in arms, offer gambling services or are VASPs. Nor do they offer correspondent services, except to subsidiaries. This supports a good risk understanding since it

allows banks to focus on familiar activities where risks are understood. Following changes to the CC, the majority no longer offer services to shell companies given the higher risk that they may be used in schemes to perpetrate tax offences, or have customers linked to states with strategic deficiencies. Some do not offer services to foreign PEPs.

422. Banks treat private banking and wealth management, including structures used, and cash intensive activities as high-risk bearing (but these may not always trigger EDD measures). These are in line with the risk landscape of the country. In line with the DDA, they would always assign high risk to: (i) PEPs; (ii) complex structures; (iii) persons or BOs domiciled in states with strategic deficiencies and countries with increased geographical risk according to List A of FMA Guideline 2013/1 on the risk-based approach; and (iv) cross-border correspondent banking. Banks mostly assign low risk to natural persons from German-speaking countries (Liechtenstein, Germany, Switzerland, and Austria) who are retail clients, where account turnover does not exceed pre-determined thresholds and there are no other criteria for increased risk. Such methodologies are considered to be fair and sound.

423. FMA inspections have shown that there were important weaknesses regarding the understanding and acknowledgement of risks at the time of NRA I (covering the period from 2013 to 2015). From a methodological point of view, inherent risk was often assessed net of the effect of mitigating measures, which caused inherent risk to be underestimated at several banks. Risk understanding and acknowledgement in the banking sector has improved significantly since supervisory measures were strengthened in 2019, something confirmed in interviews with the banking sector.

424. Banks have implemented a risk-based approach whereby customer risk assessments are prepared taking account of: (i) the BRA; (ii) risk factors listed in internal instructions and in Annexes 1 and 2 of the DDA; (iii) the Risk Factors Guidelines of the European Banking Authority; and (iv) the results of the NRA. When assessing customer ML/TF risk, banks consider: (i) customer risk; (ii) geographical risk; (iii) product/service risk and transaction risk; and (iv) distribution channel risk. Risk assessments are updated on an ongoing basis, generally for low risk every 5 years, for normal risk every 2 to 3 years, and for increased and high risk every 1 to 2 years. Risks are also updated when there is a trigger event. Such methodologies are considered to be fair and sound. They have defined clear criteria to identify the risk of business relationships and generally use four risk categories to quantify risk (low, normal, increased, and high).

425. Banks are aware of products and services that are more vulnerable in the TF context and can articulate how these products could be used for TF purposes. The understanding of trends and typologies of small banks is mainly based on indicators outlined in the annex of the DDO. Banks were also aware of the risks presented by NPOs and TF risks set out in NRA-TF.

426. Almost all banks were involved in the process of NRA II, mainly through filling in a risk questionnaire shared by the authorities and giving feedback on an advanced draft. Generally, most banks agreed with the risks identified in NRA II and found the assessment helpful, though, in most cases it did not lead to significant changes in the BRA and CRA process, as these risks were already reflected in internal instructions. Several banks mentioned that deeper analyses of threats and vulnerabilities in the sector would be appreciated.

427. All banks demonstrated a sophisticated understanding of their AML/CFT obligations and of their own AML/CFT policies and procedures. Banks' understanding of AML/CFT legal

obligations is higher than that of other FIs. Banks demonstrated a good understanding and advanced practical knowledge of their TFS-related obligations. They were clear on their respective obligations related to identification, freezing, and reporting of TFS-related cases.

Non-banks FIs

428. The understanding of ML/TF risks in non-bank FIs (including investment funds and asset managers) is also good, but less robust than for banks and varies among different entities. Whilst most non-bank FIs have conducted a BRA, there was less understanding of business specific risks and some small non-bank FIs struggled to articulate the TF risks presented by products offered by them and how their institution could be misused for ML/TF purposes. FMA inspections show that, in some cases, BRAs are still not sufficiently detailed and, like in the banking sector, inherent risks have been assessed in part taking mitigating measures into account and are thus underestimated.

429. Most non-banks FIs (including investment funds and asset managers) had a risk appetite statement which limits activities to core wealth management areas, e.g., excludes customers in the defence sector or which trade in arms. This allows them to focus on familiar activities where risks are understood. In line with the country's risk landscape, some have also restricted business relationships connected to states with strategic deficiencies. All non-bank FIs identified cash transactions as an area of increased risk. In line with the DDA, non-bank FIs generally described high-risk customers as those involving: (i) PEPs; (ii) complex structures; and (iii) persons or BOs domiciled in states with strategic deficiencies and countries with increased geographical risk according to List A of FMA Guideline 2013/1 on the risk-based approach. Additionally, insurance undertakings consider HNWIs as presenting increased risk.

430. Non- bank FIs (including investment funds and asset managers) assess the risk of each customer (mainly low, medium, and high) using the same risk factors as banks when assessing customer risk. Like banks, the frequency of risk assessment updates depends on the risk of the business relationship. At the time of NRA I, FMA inspections highlighted important weaknesses in risk assessments, e.g., risk factors were often not adequately weighted or overlooked, which lead to an increased number of low-risk business relationships. This has been addressed after supervision was strengthened in 2019.

431. In cases where non-private investment funds do not identify underlying investors (exemption under Art. 22b of the DDO), it is not possible to fully understand the risk that is presented by those investors (whose units are held through a subscribing bank acting as an intermediary). However, the application of this exemption by investment funds is risk-based and so this should not materially affect risk understanding.

432. All non-bank FIs are aware of the findings of NRA II, but their degree of involvement in the NRA process varied. Most agreed with the risks identified and agreed that the assessment would help them to improve their RBA.

433. Most non-bank FIs (including investment funds and asset managers) demonstrated a generally good understanding of their AML/CFT obligations, reflected in internal AML/CFT policies and procedures. Understanding of TFS-related obligations in non-bank FIs was generally good, but less robust than in the banking sector.

DNFBPs

434. DNFBPs' understanding of ML/TF risks is generally good but less robust than in the banking sector. Some DNFPBs (especially large TCSPs) have a better understanding of risks than non-bank FIs. Overall, TCSPs and casinos have a better understanding of ML/FT risks, but it varies according to the size of the organisation.

435. Most TCSPs have prepared a BRA and have a risk appetite statement. They periodically identify, assess and review their exposure to ML/TF risks taking account of products/services offered, customer base and relevant contextual factors. Methodologies followed are fair and sound, but FMA inspections have shown that TCSP BRAs have not always been robust enough and need strengthening. Most TCSPs limit activities to the use of legal persons and legal arrangements for core wealth management areas which allows them to focus on familiar activities where risks are understood, and would not offer their services for other purposes, e.g., to persons involved in arms trading, the pharmaceutical sector or VASPs. All are familiar with the risks that complex structures of legal persons and legal arrangements present and with offering only "limited services" to legal persons, e.g., registered office only service, where the TCSP does not proactively engage in management and/or oversight of entity activities. Most do not provide services to persons connected to states with strategic deficiencies or (following recent changes to the CC) establish shell companies (which may be used in schemes to perpetrate tax offences), and some have extended restrictions to high-risk and African countries. This is considered to be in line with the country's risk landscape. TCSPs generally described high-risk customers as those involving: (i) PEPs; (ii) complex structures; and (iii) persons or BOs domiciled in states with strategic deficiencies and countries with increased geographical risk according to List A of FMA Guideline 2013/1 on the risk-based approach.

436. Customer risk is assessed based on: (i) DDA/DDO requirements; (ii) a BRA template published and developed by the Institute of Professional Trustees in collaboration with the FMA; (iii) a CRA template developed by the FMA jointly with the private sector; and (iv) outcomes of the NRA. Risk assessments take the following factors into account: (i) customer risk; (ii) geographical risk; and (iii) product risk. Contextual factors are also taken into account. Updates are done on an ongoing basis according to risks. These methodologies are considered to be fair and sound. FMA inspections have shown that the economic sense or purpose of a business relationship has not always been sufficiently questioned in individual customer risk assessments.

437. All TCSPs met onsite noted that they either do not have low risk customers or the numbers of such customers are insignificant. This is reasonable given Liechtenstein's position as an IFC. Nevertheless, this position is different to the one shown in NRA II – which identifies that around 17% of customers had been classified as low risk (2018). The reason for this is a combination of shortcomings in the customer risk assessment (CRA) process and some initial data collection issues. Like for FIs, this percentage has gradually decreased because of strengthened supervisory measures since 2019 and resolution of data collection issues.

438. TCSPs are aware of products and services that are more vulnerable in the TF context and can articulate how these products could be used for TF purposes. The understanding of trends and typologies in large TCSPs is at the same level as in banks. In small TCSPs the understanding is less robust than in large entities and mainly based on indicators outlined in the annex of the DDA.

439. TCSPs are aware of the findings of NRA II, but their degree of involvement in the NRA process varied. Most TCSPs agree with the risks identified, of which they say they were already aware.

440. Most TCSPs demonstrated a generally good understanding of their AML/CFT obligations, which are reflected in their internal policies and procedures. The understanding of obligations in large TCSPs was better than non-bank FIs. Understanding of TFS-related obligations and practical knowledge of this issue in large TCSPs was on same level as in banks.

441. The understanding of ML/TF risks in other DNFPBs is less sophisticated, but at a satisfactory level. Casinos and real estate agents demonstrated a good understanding of ML/TF risks and were aware of the NRA results, however, one casino had not yet prepared a full scope BRA including an assessment of risk appetite. This is assessed as a minor deficiency by the AT, because of the small size of the casino which had only a few months of operational history. Understanding of risk by lawyers and accountants was less developed, given limited engagement in regulated activities, but at a satisfactory level. Risks in the legal sector are limited. Where they provide advice on structuring or formation of legal persons and legal arrangements, then they do so under the umbrella of a TCSP (and not as a lawyer), and they are not directly involved in transactions concerning the buying and selling of real estate, where their role is limited to providing standard contracts.

442. The understanding of AML/CFT obligations in other DNFPBs is less sophisticated, but at a satisfactory level. Casinos and real estate agents demonstrated a good understanding of AML/CFT obligations. Understanding of TFS-related obligations was generally good, but less robust.

VASPs

443. Understanding of ML/FT risks in the VASP sector, which is dominated by one large provider, is generally good and large VASPs have a better understanding of their ML/TF risks. VASPs met during the onsite visit assess business and customer risk, but FMA inspections indicate that some VASPs are still in the process of refining the former. VASPs systematically identify, assess, and review their exposure to ML/TF risks using the same factors as set out above. Large VASPs have produced risk appetite statements and do not offer services to sectors with reputational risk, e.g., adult industries and arms traders. To reduce risk most of them do not offer services to PEPs or states with strategic deficiencies. As the "travel rule" is not implemented globally yet, it is not possible to have sufficient information about the beneficiaries of VA transfers, which prevents a full analysis of the risks.

444. VASPs generally divide their customers into three or four risk categories, but do not have low risk customers because of the requirements of the DDA. The majority are classified as high-risk bearing. Given the risks of the sector highlighted in the NRA, difficulties obtaining full CDD information on legacy customers and obstacles in practical implementation of the travel rule, the AT considers this to be reasonable.

445. Large VASPs are aware of products and services that are more vulnerable in the TF context, but the understanding of trends and typologies is less robust than in the banking sector.

446. Understanding of AML/CFT obligations in the VASP sector is generally good. Large VASPs have a better understanding of AML/CFT obligations. As for smaller VASPs, their understanding is less developed, something highlighted also in FMA findings on the BRA process.

5.2.2. Application of risk mitigating measures

447. FIs, DNFBPs and VASPs have implemented AML/CFT preventive measures to mitigate their ML/TF risks. The extent to which these preventive measures are applied varies between, and within, these sectors.

Financial institutions

448. Banks have developed sophisticated AML/CFT systems and controls. Their AML/CFT policies and procedures contain a broad range of measures, including ongoing monitoring to mitigate ML/TF risks. They typically apply preventive measures commensurate to the risk. They build up business profiles for clients according to the requirements of the DDA and DDO which are reviewed on an ongoing basis – frequency depending upon assigned risks. For increased and high-risk customers more scrutiny is applied, such as obtaining approval from general management, requesting more information and documentation about the client/BO, including on SoW and SoF, and more frequent reviews of customer files. Non-bank FIs have also developed similar AML/CFT systems but have generally less robust and sophisticated AML/CFT controls (including monitoring) compared to banks.

449. Given the country's focus on private banking and wealth management for non-residents, strong measures to establish SoW and SoF are being applied by all FIs. Liechtenstein applies a stricter approach than is required under R.10, by requiring information to be collected on the background of contributed assets and on total wealth for all customers. In the case of increased and high-risk customers, this information is then verified based on reliable documents. This means that customer profiles tend to be comprehensive even for low and medium risk relationships, though sources for contributed assets and wealth will often be similar in such cases, e.g. employment (which means that a disproportionate burden is not placed on lower risk customers). The amount and level of detail of SoW and SoF information depends on the risk involved: less detailed information and no corroboration is required for low-risk customers and detailed information and corroboration is required for higher risk customers. The AT considers that the above-mentioned approach is commensurate to the risks of the jurisdiction.

450. The general improvement in measures taken to establish and corroborate economic background of SoW and SoF is observed mainly after FMA supervisory measures were strengthened in 2019. Information on SoW and SoF is not collected by non-private investment funds on underlying investors when applying the exemption under Art. 22b of the DDO.

451. In the insurance sector (assessed as presenting a medium-high inherent risk), customer acquisition usually involves a delegated insurance intermediary that is responsible for identifying and verifying the identity of the contracting party/customer on behalf of the insurance undertaking. However, to address this risk, such undertakings explained that they never rely solely on the intermediary and, as a rule, they conduct their own additional review of received documents as a necessary step for the final decision on whether to enter into business relationship. In addition, systems and controls of intermediaries are mostly assessed based on responses to questionnaires. These measures are commensurate with risk.

452. As for investment funds (assessed as presenting a medium-high inherent risk), where underlying investors in non-private investment funds have not been identified (exemption under Art. 22b of the DDO), policies and procedures for subscribing banks are not always considered to assess risk. Nor is information on the profile of underlying investors routinely reviewed, including incidence (if any) of SARs/STRs and asset freezes under TFS. Additionally, it was not demonstrated to the AT how CDD information on underlying investors could be obtained without delay, if needed. Overall, the application of mitigating measures by investment funds is not always conducted according to the requirements of Art. 22b of the DDO and therefore is not always considered to be commensurate with risk.

453. All banks and non-bank FIs identified cash transactions as an area of increased risk. Banks apply additional preventive measures to mitigate these risks, such as: (i) setting thresholds for cash transactions (CHF 10 000 to CHF 100 000), beyond which there are additional questions and requests for documentation to explain the SoF; (ii) checking plausibility of cash transactions with business profile; and (iii) four-eyes approval from line management. Some banks also do not conduct cash transactions with NPOs. Insurance undertakings do not accept cash. Whilst these measures are considered to be commensurate with risk, setting upper limits on cash transactions is not a common practice amongst banks, which could be an important additional preventive measure.

454. NRA II highlights risks presented using shell companies, and an amendment in 2019 to the CC (Art. 165) has significantly raised the stakes in this respect. Banks announced that, as of the date of the revision coming into force, they would regard business relationships involving the use of supposedly active companies (production, trade, or services) without physical substance as potentially fraudulent. As a result, all FIs have improved their control systems to detect and monitor such companies and banks have sought to exit relationships (which are not acceptable according to their risk appetite statements). For relationships with companies, banks now always consider economic substance, including: (i) collecting information about the number of employees and requesting employment contracts; (ii) checking audited financial statements and tax declarations to be sure that company is tax compliant; (iii) requesting rental and ownership documents for premises and, if needed, making on-site visits to check that the space is consistent with the business profile of the customer; and (iv) checking information about major business partners of the customer. These are important controls and mitigating measures are in line with risks identified.

455. One bank explained that they had closed accounts for almost one third of their customer base, because customers did not provide the necessary information/documentation to support economic substance. Despite the high number of closed accounts, only a few closures led to submitting of a SAR/STR to the FIU. Other banks reported lower numbers of closures. The authorities explained that they had seen a significant loss in business but could not quantify this and had not analysed funds outflows after relationships had been closed, e.g., value and destination. This is considered more under Chapter 2 (IO.1). However, banks stated that they had limited outflows strictly to accounts in the same customer's name.

456. In a case when a legal person or legal arrangement is considered to have a "complex structure", FIs take effective measures to address risks presented by such customers by applying EDD measures and requesting information/documentation about a customer's group structure to be able to understand the whole structure, its risks and identify each layer and the BO of the

structure. These mitigating measures are commensurate with risks. Despite this, and even though the FMA has published guidance to define several factors that must be considered when determining whether a structure is complex or not, understanding of complex structures, even in very similar cases, differs across FIs, which, is leading to uneven implementation of enhanced measures. Whilst most defined "complex" as a structure of three or more layers of ownership, others introduced other factors into their definition, e.g., use of several different jurisdictions and other risk factors e.g., country risk.

DNFBPs and VASPs

457. All DNFBPs and VASPS have developed AML/CFT systems and controls, including monitoring processes. Their AML/CFT policies and procedures include different measures to mitigate ML/TF risks, but the level of application is uneven across sectors and types of DNFBPs.

458. Large TCSPs, casinos and VASPs have more well-structured risk management systems, then other smaller ones.

459. Large TCSPs demonstrated the most varied and sophisticated risk mitigation strategies. When considering a potential new client, generally, large TCSPs follow a similar approach to banks. Like banks, they build up a business profile for their customer, which is updated based on risk. For increased and high-risk customers more scrutiny is applied, in line with examples given above for banks. TCSPs always request information about SoW and SoF and in a case of high risk, more in-depth verification is conducted based on documents issued by third parties, e.g.: audit reports, tax declarations, dividend distribution decisions, contracts that prove the sale of goods, and certificates of inheritance. TCSPs also check publicly available information to consider the plausibility of the SoW of the customer and BO. Given that the TCSP customer base is primarily non-resident, the AT considers this approach to be commensurate to the risks of the jurisdiction and a valuable mitigating measure. FMA inspections show that the quality of this process has gradually improved in recent years (mainly after supervisory efforts from 2019), but there is not yet consistency in approach across the sector as information held on SoW is sometimes limited, especially in the case of legacy customers. This was also confirmed during meetings with the sector, as some TCSPs mentioned that establishing and corroborating total net worth of the customer or its BO, especially in the case of legacy customers, is quite challenging and, sometimes, almost impossible.

460. The approach of TCSPs regarding complex structures is the same as in the banking sector, though TCSPs have the advantage of being closer to the structure and involvement in establishing it. To understand the economic purpose of such structures, which present a higher risk, they request all necessary information. Some TCSPs, but not all, will involve tax advisors (perhaps in-house) to understand the tax benefit of using a structure and to confirm that their customer is tax compliant. TCSPs also use publicly available sources to get information about underlying companies in the structure. Whilst these mitigating measures are commensurate with risk, the AT consider that additional importance should be attached to obtaining advice on foreign tax compliance in case of higher risk, since tax is often a key driver for complexity. Like in the banking sector, there is no single view on what is complex, and decisions are made case by case. One TCSP explained that, if they fully understand the company's ownership structure, they will not treat the structure as complex, irrespective of the number of layers or countries involved. Such an approach would limit the application of EDD measures. Other DNFPBs also have differing views on what is complex.

461. To address the risk that companies may be used in schemes to perpetrate tax offences, TCSPs now always ask for information/documentation (both during onboarding and through ongoing monitoring) to check the substance of the proposed corporate activities, e.g., financial statements, tax declarations and other reliable documents issued by the third parties. This is considered to be an appropriate risk mitigation measure. The effect of this measure is that consistent with explanations provided by banks, shell companies are no longer used by domestic TCSPs to any great extent. Despite this, few were able to provide approximate numbers of terminated business relationships with shell companies based on identifying insufficient economic substance.

462. A key strength of the legal system for legal persons is a requirement for legal persons to appoint a qualified member to sit on the governing body (Art. 180a) of the Persons and Companies Act) (there are some exceptions, but they are not relevant here) which means that a TCSP will be engaged in day-to-day management and/or oversight of that entity's activities. This significantly reduces the risk that administered structures may be abused. TCSPs confirmed that such qualified members are actively involved in the decision-making process for the legal person, and that, as they are personally responsible for activities of the company, will have full knowledge of underlying activities. In the context of such a regime, there is no opportunity to provide more limited services to legal persons (e.g., provision of a registered office address) and TCSPs identified that, in any case, it would not be economic to do so. Nevertheless, the NRA identifies the risks involved in granting customers individual signing rights, e.g., powers of attorney, so that they might independently carry out transactions or, in fact, administer the legal person themselves – thereby reducing the mitigating effect of the Art. 180a mechanism. TCSPs are aware of these risks and noted that such practice is hardly ever observed in the sector, as it is rare now to give a power of attorney to another party.

463. Risks for casinos are effectively mitigated. Casinos do not: (i) offer player or guest accounts; (ii) issue winning cheques or wire transfers of winnings; or (iii) issue winning confirmations. Whilst currency exchange is offered (EUR to CHF, but not vice versa), it is assessed as bearing high risk, and so thresholds are in place over the amounts that may be exchanged, which trigger the need to prove SoF. There are controls in place to limit this exchange service only to customers of the casino. These measures are commensurate with risks.

464. Application of risk mitigation measures (including monitoring systems) in other DNFPBs is less strong, but still satisfactory, as measures taken manage the risks they face from their clients and offered products and services.

465. VASPs have also developed different risk-based measures to mitigate ML/TF risks, e.g., different tools to analyse transaction chains to detect suspicious activity and stop customers using mixers, tumblers or the darknet. Restrictions have also been placed on coins with a high level of anonymity. Information received during onsite meetings indicates that VASPs are using a wide range of risk mitigation measures that are commensurate with risk. However, the fact that the "travel rule" is not yet fully applied in practice, as well as challenges in the application of risk-based preventive measures to legacy customers at one large entity, both in terms of the renewal of CDD documents and gathering sufficient information about SoW and SoF, affects the full implementation of preventive measures. Whilst the accounts of legacy customers without proper CDD have been blocked, it seems that this was the result of supervisory intervention rather than risk mitigation by the entity itself.

5.2.3. Application of CDD and record-keeping requirements

FIs

466. All FIs demonstrated generally good knowledge of applicable requirements and regulations related to CDD and record keeping. All FIs apply risk based CDD measures, including ongoing monitoring. The approach of banks is more comprehensive than for non-bank FIs. All FIs met during the onsite visit demonstrated that they have CDD procedures in place and, according to the risk of the business relationship, they use different reliable information/documentation to identify/verify the customer and its BO. Irrespective of risk, the business profile of the customer now contains information about SoW and SoF (mainly following the strengthening of supervisory measures in 2019) and purpose and intended nature of the business relationship.

467. Whilst the information on customer identity obtained by FIs to identify the contracting party/customer is largely similar for all risk classes, they are guided by the risk profile of the customer when determining the type of documents to be used for the verification of identity. Irrespective of risk, FIs demand additional documents to verify the current place of residence of the client (e.g., utility bill or confirmation of residence). In the case of a customer that is a legal person or legal arrangement, FIs obtain an ownership and corporate structure chart to understand that structure and to identify the natural person(s) who ultimately owns or controls the customer. In the case of a customer that is trust, FIs request to see the trust deed and collect information about the trustee(s), settlor, and beneficiaries. Most of the banks mentioned that, in the case of increased/high risk, they try to have a face-to-face meeting with the BO. However, this cannot be considered as an established practice in the sector.

468. Where relationships are established remotely (i.e., no physical contact with the customer), FIs apply additional safeguards like "suitable certification" where identification measures are applied through a trusted external party and where the customer (or other person) is seen on a face-to-face basis by that trusted external party. Video identification of non-resident customers is offered only by one bank to a limited extent and only to natural persons domiciled in Liechtenstein or neighbouring German speaking countries.

469. Generally, FMA inspections and AT meetings with FIs show that they have comprehensive procedures to identify and verify the BO of the client. In addition, it is clear that, in accordance with legal requirements, FIs also identify and verify all persons acting on behalf of the customer.

470. Banks have implemented systems for: (i) screening CDD information against external commercial databases (sanctions, adverse media or other information etc.); and (ii) scenario-based transaction monitoring. For (i), banks mainly use automated, IT-based systems (e.g., World-Check, Pythagoras, etc.). This also includes event-based press screening like updating of business profiles. Banks have implemented IT software to monitor transactions on an ongoing basis in order to pick up those that meet certain scenarios/criteria and, where there are anomalies, to generate an alert which starts an investigation according to the requirements of the DDA. Banks are using both ex-ante (e.g., for list matching) and ex-post monitoring (e.g., the analysis of circumstances or transactions that deviate from the business profile) tools. Banks were able to generally demonstrate that they have a good understanding of parameters and typologies used to set scenarios and criteria.

471. Insurance undertakings and investment funds and asset managers, like banks, have also implemented IT monitoring systems, but these systems are less sophisticated and robust, and, in some institutions, systems are not automated.

472. In the insurance sector, undertakings are identifying and verifying the identity of beneficiaries of life insurance policies. Where the beneficiary is a legal person, the BO of that legal person is identified and verified. In the case of the investment fund sector, fund unit subscriptions are nearly all made by banks, and so underlying investors in non-private investment funds are rarely identified or verified. However, application of this exemption (DDO, Art. 22b (3)) is contingent upon: (i) application of risk-based measures to ensure that ML/TF risk is low; and (ii) an examination of the internal control and supervisory measures of the subscribing institution. It is not clear to the AT that these elements are being considered and addressed in every case (see section 5.2.2 above). Nor is it clear how CDD information on underlying investors would be obtained without delay, if needed, from the subscribing institution. The confidentiality of such information was mentioned as a possible obstacle by some fund and asset managers. In a case where an investment fund which is using the exemption under Art. 22b of the DDO is itself a customer of another FI, e.g., asset manager, that FI is not in position to find out in every case whether there is any individual owning more than a certain percentage of the fund as this information is not held by the fund itself. This cascades the effect of the exemption into other sectors.

473. It does not appear that full CDD information has been held throughout the period under review. Whilst FIs are now applying CDD measures effectively (except as noted above), some mentioned improvements to their systems in the past two to three years, to remediate business profiles and information held about the BO (see below) and on SoW and SoF - identified internally or through the FMA. For some, remediation of information held remains ongoing, which means that quality of the CDD measures conducted by FIs was not consistent during the assessed period and has gradually improved.

474. In particular, following the introduction of an expanded definition for the BO of a foundation or trust, FIs were required to update information held for all existing business relationships with regard to the settlor, trustee, and protector (or equivalent). FMA inspections have shown that all FIs concluded these examinations for business relationships with high and increased risk by the end of 2018. Other business relationships were completed by the end of 2020. For some of the period under assessment, FIs did not have up to date information on tax residence for settlors and protectors.

475. Some FIs, including banks, have refused to establish, or have terminated, business relationships where they have not been able to complete the CDD process and considered whether to file a SAR/STR with the FIU. Nevertheless, the number of SARs/STRs filled in such cases are low.

476. CDD information is generally updated by all FIs in line with DDA and FMA guidelines. The frequency depends on the risk level assigned to the client, usually one to two years for high/increased risk customers, two to three years for normal risk customers, and five years for low-risk customers.

477. All FIs are keeping records for the necessary ten-year period.

DNFBPs and VASPs

478. DNFBPs and VASPs demonstrated generally good knowledge of applicable requirements and regulations related to CDD and record keeping. The extent to which CDD and record-keeping requirements are implemented varies and is based on risk. All DNFBPs and VASPs met during the onsite showed that they have risk based CDD procedures in place. Irrespective of risk, the business profile of the customer now always contains information about SoW and SoF (mainly following the strengthening of supervisory measures in 2019) and purpose and intended nature of the business relationship. As highlighted under section 5.2.2, there remain issues in profiling SoW for TCSPs.

479. TCSPs are performing CDD on the BO of legal persons and legal arrangements and have direct contact therewith. The process followed is set out in internal procedures and FMA inspections show that, in general, measures applied are in line with the DDA and DDO. Given that TCSPs are involved in the establishment of legal persons and legal arrangements, they have first-hand knowledge of the structures used by their customers. In a case of high risk, additional documents are requested. No TCSPs conduct CDD by means of video or remote identification. Although Liechtenstein TCSPs may sometimes obtain the necessary due diligence information and documents from third parties (e.g., via introducers), they carry out their own preventive measures necessary for the onboarding process.

480. Most TCSPs use IT systems to monitor their business relationships in a risk-appropriate manner. These systems differ according to the size of the TCSP, as large TCSPs have more sophisticated and automatic systems, while small ones monitor relationships manually. In these cases, thresholds are set, above which investigations of transactions are carried out or all transactions are subject to a brief plausibility check to ensure that it is in line with the business profile held. Since TCSPs are usually involved in instigating transactions, this makes it easier to identify deviations from business profiles before transactions are executed. However, FMA inspections show that, in some cases, there is a lack of depth in ongoing monitoring as some TCSPs appear to pay too little attention to the business relationship as a whole and instead are looking only at individual transactions in isolation.

481. TCSPs were required to review information held for all existing business relationships by the statutory deadlines regarding settlor, trustee, and protector (see above). TCSPs concluded these reviews for business relationships with high and increased risks by the end of 2018. Other business relationships (without high or increased risks) had to be completed by the end of 2020. FMA inspections showed that this review was carried out by the deadlines laid down in the transitional provisions. In some cases, TCSPs completed the review of their entire mandate portfolio by the end of 2018 or 2019, ahead of time.

482. Some DNFPBs have refused to establish, or have terminated, business relationships where they have not been able to complete the CDD process and have considered whether to file a SAR/STR with the FIU. Nevertheless, FMA inspections have identified some isolated instances where TCSPs did not terminate an existing business relationship immediately, but rather tried for too long to obtain the missing CDD information.

483. Unlike for other sectors, the majority of customers of VASPs are natural persons, where significant use is made of remote and video identification. Verification of identity is generally done on the basis of authenticated copies of passports or identity cards with photograph. The

video identification tools used also check the authenticity of identity documents to reveal forged documents.

484. VASPs use scenario-based automated IT and different chain analysis systems for tracing transactions and detecting suspicious transactions. Despite the fact that IT tools used by large VASPs are sophisticated, the lack of adequate customer profiles (e.g., up to date identification documentation and information about SoW and SoF) for legacy customers at one large entity, which has a dominant position in the VASP sector, and absence of practical implementation of the travel rule has impacted to some extent on effectiveness of monitoring systems during the assessed period.

485. All DNFBPs and VASPs are keeping records for the necessary ten-year period.

5.2.4. Application of EDD measures

PEPs

486. The Liechtenstein legal framework covers both foreign and domestic PEPs, but, until September 2021 included some legislative shortcomings (see R.12). In practice, the majority of persons subject to the DDA do not apply a fixed "cooling off" period and PEP status is removed only in a case where, based on substantiated analysis, there is no longer a risk associated with PEP status. Accordingly, it is considered that the legislative shortcoming in this regard does not have a negative impact on effectiveness of measures.

487. FIs, DNFPBs and VASPs have adequate measures in place to determine whether the customer and/or the BO is a PEP. Checks also cover recipients of distributions and all authorised signatories. They ask for approval from general management before establishing or continuing business relationships, establish SoW and SoF based on reliable information/documentation issued by third parties, and apply enhanced monitoring (with lower thresholds). All categories of PEPs are assigned a high risk and EDD measures are applied, but these are more granular and enhanced in the case of foreign PEPs.

488. Most use commercial databases (e.g., Pythagoras, World-check, etc.) and automated screening programmes to identify PEPs. Only small DNFPBs are doing screening manually. In order to highlight new PEPs in existing relationships, rescreening is done at regular intervals: in some cases, it is done daily or automatically when lists are updated, or at least every month. There is a check that commercial databases used cover domestic PEPs. Public sources are also checked to identify any PEPs that are not recorded in commercial databases. It is also common practice amongst FIs to obtain a self-declaration about PEP connections.

489. Based on supervisory findings, the FMA has evaluated positively the measures taken to apply CDD requirements to PEPs, though it is noted that business profiles of legacy customers are less detailed than those for more recent relationships and, in some cases, getting full information about SoW is challenging even in the case of a PEP.

Opening and maintaining correspondent relations

490. Liechtenstein banks do not provide correspondent banking services. Only two banks provide intra-group correspondent banking services for their foreign subsidiaries.

491. With regard to intra-group correspondent banking services, parent banks collect sufficient information about the subsidiary bank (respondent institution) to fully understand the

nature of its business activities and to be able to assess its reputation and the quality of supervision. Management approval is always required to start such correspondent relationships and responsibilities of each institution are clearly documented. There is ongoing monitoring of the business relationship, including post-execution monitoring of transactions.

492. Historically, one small bank with an increased risk profile had a relationship which should have been classified as a correspondent banking service, but which was not treated as such. Based on supervisory actions, this relationship was terminated.

493. Correspondent-type relationships are found in the VASP sector, e.g., relationships with exchange service providers which offer accounts to commercial clients. VASPs are applying EDD measures with regard to correspondent relationships but it is not clear if the measures applied are in line with R.15/R.13 as some institutions with whom VASPs are in correspondent relationships are not subject to AML/CFT supervision.

New technologies

494. Persons subject to the DDA conduct risk assessments before using new and developing technologies - prior to the launch of any new business/product. If needed, BRA and customer risk assessments are also adjusted, e.g., to reflect changes to risk introduced by fintech, but based on supervisory experience, this approach is mainly observed in large entities. In addition, it should be noted that use of new technology is not widespread in the DNFPB sector.

495. Compliance officers plays an important role in the assessment process, by ensuring implementation of due diligence obligations when new technologies/products are introduced. Overall, AML/CFT risks are identified, evaluated and risk mitigation measures are developed.

Application of wire transfer rules

496. Wire transfer services are provided through: (i) banks; (ii) e-money institutions; (iii) an MVTS operator (agent under EEA passporting regime); and (iv) VASPs (VA transfers). Except for VASPs, all wire transfer information (incoming and outgoing) is screened by systems to make sure that it contains all required data. In cases of missing information, an investigation is conducted which includes communication with the originating institution to ask for additional information. This process is done before proceeding with the transfer. If the missing data is not supplied, the payment will be returned to the originator (in the case of an incoming transfer) or execution of the payment is rejected (in the case of an outgoing transfer). Checks on data are also carried out periodically post transfer. The requirements under R.16 are followed in practice.

497. In practice, the "travel rule" is not implemented yet in the VASP sector, which is partly due to the absence of global implementation of the travel rule. This is one of the biggest challenges for the VASP sector. One large VASP, which has a dominant position in the sector, noted that it has already started working on implementation of the "travel rule" under the supervision of its parent company and expected to do so at the end of the 2021. Meanwhile, it has established thresholds for transactions which generate alerts if incoming transfers come from an unknown VASP. Based on information provided by the authorities, VASPs are using different systems to implement the travel rule, for instance "Notabene" or "21Analytics", but this was not confirmed by the VASPs met onsite, which mainly are using "in-house" solutions to implement the travel rule.

Implementation of Targeted Financial Sanctions

498. Persons subject to the DDA screen for potential TFS before the establishment of a business relationship or conducting transactions (but see comment below on VASPs). Many use commercial databases from third-party vendors (as for PEPs) to screen: (i) their customers and BOs; (ii) authorised signatories; and (iii) transactions, against lists of persons and entities designated under UNSCRs, domestically and in other countries, e.g., OFAC, the EU and in Switzerland. In most sectors, screening is automated, but those with small customer bases mainly carry out list screening manually. The frequency of re-screening differs according to sector: banks screen their database at least weekly (some daily). In other sectors, screening is performed immediately after notification of list changes by the FIU and at monthly to quarterly intervals. Whilst the authorities have developed "red flags" related to cases of suspicion of TF, understanding of most persons in relation to TFS is limited to checking existing lists.

499. Some banks and large non-bank FIs use fuzzy matching and transliteration programs which have the ability to reveal matches even in case of spelling mistakes. The authorities have highlighted difficulties in detecting persons indirectly controlling or owning funds concerned in transactions.

500. When there is a match, an investigation is opened to understand whether it is a false or true positive. In a case when information is missing in a screening programme, public sources or other external investigation tools are used. Whilst reports of matches have been sent to the authorities, these have not been linked to domestic implementation of relevant UNSCRs. Generally, the number of matches is small and mainly false positives. Most persons subject to the DDA explained that they would refuse completion of a transaction and would file a report to the FIU in case of a match. However, they were less clear on what would be done in case when, irrespective of a match, there is a suspicion of TF.

501. In investment funds, widespread use is made of an exemption pursuant to the DDO under which information is not held on underlying investors of non-private investment funds. Accordingly, TFS screening in relation to these underlying investors is conducted only by subscribing banks and, in the case of a match, assets frozen only by the subscribing bank. Arrangements are not in place for the subscribing bank to report the fact that there has been a match, though this is relevant to continued use of the exemption.

502. FIs and TCSPs are familiar with long-standing guidance, which addresses major aspects regarding TFS. However, some small and medium-sized persons subject to the DDA were not able to explain exactly what new requirements had been imposed by a new TFS guideline issued more recently by the FIU.

503. In the case of VASPs, as the "travel rule" is not implemented yet in practice (partly due to the absence of global implementation), information about payer/payee is not screened properly and VASPs focus on screening their customers and opened wallets. Blockchain TFS screening currently follows a different logic: wallets/blockchain addresses can be blacklisted/red-flagged, not persons, entities, or activities. Although this is a global problem, the AT has concerns in this regard especially due to the significant volume of transactions carried out through the sector.

Approach towards jurisdictions identified as high-risk

504. Persons subject to the DDA check their customer base (customer, BO, authorised signatories) and payment transactions (payer and payee) to identify any that have a nexus to countries with strategic deficiencies (which includes countries subject to a call from the FATF).

Where there is a match, they do not proceed with a relationship or transaction (e.g., it is outside their risk appetite) or they apply EDD measures.

505. No links to North Korea were identified. During the period under review, two small banks held business relationships with a notable number of customers connected to Iran. By the time of the onsite visit, one of these banks had been liquidated and the second blocks all transactions, except with the agreement of its compliance function.

506. Enhanced information/documentation is requested to support: (i) customer profiles (SoW of the customer/BO); (ii) the purpose and nature of transfers, including SoF; and (iii) identification and verification of the client/BO. Approval from general management is needed when a starting business relationship linked to such a country and an enhanced monitoring process will be applied.

507. Most persons subject to the DDA have automated systems and tools to monitor incoming and outgoing transactions which allows transactions with countries with strategic deficiencies to be flagged and followed-up. Small persons subject to the DDA do this monitoring process manually. Large FIs and DNFPBs also mentioned that their list of so-called "high risk jurisdictions" is broad and encompasses different factors e.g., countries that are subject to enhanced monitoring by the FATF, at risk of corruption or terrorism, or which have low transparency standards.

508. The possibility of identifying a nexus is limited for VA transfers (because the "travel rule" has not yet been implemented) and is not possible in respect of underlying investors in non-private investment funds (because this information is only held by the subscribing bank).

509. FMA inspections have found only a small number of cases where business relationships with states with strategic deficiencies were not adequately categorised.

5.2.5. Reporting obligations and tipping off

510. During much of the period under review, persons subject to the DDA met their reporting obligations only to a limited extent. At the time of the on-site visit, a more positive position has been observed and reasons for the significant increase in the number of reports since 2018 are set out at section 3.2.2 (IO.6).

511. Where there is suspicion of ML, a predicate offence to ML, organised crime or TF, persons subject to the DDA must immediately submit a report to the FIU in writing (DDA, Art. 17). Further to this requirement, guidance for submitting SARs/STRs to the FIU stipulates that there are no special preconditions in this respect (such as a "justified suspicion"). FIU guidance provides a list of indicators that could give rise to a report of suspicion, but the list is not exhaustive. Not all persons subject to the DDA are aware of reporting typologies or indicators.

512. Whilst noting an increase in the number of SARs/STRs since 2018 (refer to Chapter 3 - IO.6), including reports in respect of tax offences, the AT considers that there has been less reporting activity linked to tax than expected following important legislative changes: criminalisation of serious tax offences in 2016 and more recent changes to Art. 165 of the CC (and related publication of indicators of tax offences in the DDO). This view takes into account: (i) inherent risks of different sectors; and (ii) findings of NRA II, and has been reinforced by meetings with the private sector which revealed that those who had made reports to the FIU could give few or no examples of having filed SARs/STRs related to tax offences, even in those cases where

relationships with shell companies had been closed. A reason for this may be that FIs and DNFPBs were informed in advance of legislative changes in 2019, which allowed time to remediate customer bases ahead of time. Overall, the reason given by the private sector for the majority of reports was suspicion of (non-tax) fraud or embezzlement.

513. NRA II comprehensively considers levels of reporting, particularly for banks, insurance companies and TCSPs. It finds in particular that: (i) there is still a lack of verified information about the economic background of the origin of assets of legacy customers, making it difficult to identify suspicious transactions from business profiles (which are insufficiently meaningful or very generic); and (ii) there is too much reliance on third party information sources (rather than transaction monitoring). In NRA II, the authorities stated that, in some cases, there is an inclination to seek explanations and information when there is already a good basis for making a report, leading to systemic reactive and late filing, which may question the ability of the private sector to properly identify and report ML/TF-related suspicion.

514. Approximately 70% of all SARs/STRs in the FI and DNFBP sectors are submitted by banks, all of which have made reports. This is consistent with the residual medium-high ML assessment in NRA II. The principles of reporting of suspicious activity and attempted suspicious activity are now well understood by banks.

515. Banks are now also aware of the need for reports to be made promptly. In the past, general management have had the final say on whether to make a report but this is no longer seen. It was confirmed that the compliance function does not need approval from general management to file a SAR/STR. If after starting an investigation a report is not filed, this is always documented and justified. After a SAR/STR is filed, clients are assigned a high risk and, in some cases, the business relationship is terminated.

516. Banks met on-site were also able to provide the AT with examples of relevant situations where SARs/STRs were filed with the FIU. These provide evidence that reporting requirements are now being applied to a greater extent. For example, one bank filed a SAR/STR because its customer, operating through a complex structure, wished to make a transfer to a third country in respect of a fee for services rendered. However, the fee appeared over-inflated, which led to a suspicion that the customer was trying to move profit from one country to another by using fictitious agreements. Another bank filed a SAR/STR as it had suspicion that an account was being used as a "transit account" to create an additional layer in the transaction chain because in a short period after opening the bank account, its customer requested to transfer to, and receive payments from, a third country (without any business or family ties to the jurisdiction) and then to transfer money to their country of domicile.

517. With regard to insurance undertakings, the authorities concluded that, in most cases reports are triggered by positive hits in commercial databases. In the investment fund sector, the number of reports is expectedly low, because there is widespread use by investment funds of an exemption pursuant to the DDO) under which information is not held on underlying investors in non-private investment funds. This has also an impact on the asset management sector to the extent that a large portion of institutional clients are investment funds. In addition, asset managers typically see only those transactions that they initiate themselves. Reporting is done only by underlying investors (subscribing banks) to their home FIU, and arrangements are not in place for the subscribing bank to notify the investment fund of such a fact, which will be relevant to continued use of the exemption.

518. After the banking sector, TCSPs submit the most reports of suspicion. This is consistent with the sector's residual medium-high ML assessment in NRA II. The average number of reports in the TCSP sector over the past 5 years corresponds to around 25% of the annual average for banks over the same period. Like for banks, all of the necessary policies and procedures are in place and reporting obligations are well understood. Some larger TCSPs are using automated IT systems to detect suspicious activities. TCSPs were also able to provide examples of reports made, which provide evidence that reporting requirements are now being applied to a greater extent. However, the authorities have identified that the reporting behaviour in the sector is predominantly reactive, which means that TCSPs often act only after a bank has submitted a report of suspicion (disclosed to the TCSP under statutory gateways) and the sector is under-sensitised. The FMA has also identified cases of late reporting and non-reporting. It is also still the case that many TCSPs have never filed a report.

519. The number of reports for lawyers and accountants might be expected to be higher in an IFC. However, as explained above, there are only limited activities conducted by these professions that are not undertaken under the umbrella of a TCSP, reporting for which is considered separately. For casinos, it is noted that the first two were approved at the end of 2019 and residual ML risks are medium-low, so a small number of reports is expected.

520. Some smaller non-bank FIs and DNFPBs were not able to explain the main typologies and red flags characteristic to their sector. In the view of the AT, this has an impact on their ability to spot what is suspicious and may explain why so many have never filed a SAR/STR.

521. Feedback is provided on an aggregated basis by the FIU on the quality of SARs/STRs and there is close communication between the private sector and FIU. However, some persons subject to the DDA suggested that more guidance on reporting is required, particularly sector-specific indicators of suspicious activities. The AT also sees a need for more sector-specific instructions as some small entities have a very general and narrow understanding of the main typologies and red flag characteristics of their sector.

522. A number of banks and TCSPs have been reported by the FMA and the FIU to the OPP in the period under review in order to enforce the obligation to report suspicion (see section 6.2.4). This has led to a number of prosecutions and to the first conviction in 2018. This is a positive development.

523. Large VASPs have reported a high number of SARs/STRs to the FIU since coming within the scope of the DDA. In 2020, 640 reports were submitted, and more than 1 000 in 2021, and this mainly reflects the high number of customers subject to remediation measures during the period and the chain analysis tool which helps VASPs to report if there is suspicion anywhere in the transaction chain. The authorities have identified a pattern of late reporting in the sector because investigations have taken a disproportionately long time or customers given too long to respond.

524. Persons subject to the DDA generally displayed good knowledge of the obligation not to tip-off and ensure compliance by staff through internal policies and procedures and training initiatives. No issues were identified in this respect. Internal procedures contain direct restrictions on disclosure, detailed obligations of employees, ability to refrain from conducting CDD when this might alert the customer and predefined written statements that can be used

during the communication with a customer. Some were able to give examples of having filed SARs/STRs without further investigation as there was concern that this might tip-off.

525. Whilst the authorities confirmed that cases of potential tipping-off are very rare, the head of compliance of one bank was indicted by the OPP for tipping-off a TCSP in 2020 following submission of a SAR/STR. The first instance court ruled on this case in March 2021. It found that actions taken by the bank/head of compliance were unlawful and wilfully conducted. However, the defendant was acquitted by the court since the exchange of information concerned a potential client of a bank and actual customer of a TCSP. Although no general conclusion should be drawn from a single case, there would be benefit in providing clear explanations on what now constitutes tipping off.

5.2.6 Internal controls and legal/regulatory requirements impending implementation

526. FIs, DNFPBs and VASPs have generally good internal controls and procedures. They are giving high priority to AML/CFT functions to support compliance with AML/CFT requirements and measures put in place are generally effective. The internal AML/CFT controls of large FIs, DNFBPs and VASPs generally are based around three lines of defence (front-line staff, compliance, and internal audit). All persons subject to the DDA have written policies and procedures in place for the implementation of AML/CFT requirements. The internal control systems of small DNFBPs are less sophisticated than those of large TCSPs. Given their size, such entities often outsource their internal audit function to specialised external providers who have sufficient experience.

527. All persons subject to the DDA have appointed at least one member of general management who is responsible for compliance with the DDA and DDO. In most cases, the BRA and risk appetite statement of the organisation is approved by top management and sets the "tone from the top".

528. FIs which are the parent entity in a financial group (domestic and foreign) have group-wide internal controls and procedural programmes that are well documented and reviewed. Most entities are giving high priority to AML/CFT compliance functions, which are properly structured and resourced and are subject to internal audits.

529. Persons subject to the DDA have screening programmes for new employees. The FMA has identified a small number of cases in small institutions where these requirements have not been adequately implemented. Most FIs, DNFBPs and VASPs also have training programmes for new recruits, management with responsibility for compliance with the DDA, and for employees in each of the lines of defence. Training differs according to the responsibilities and functions of employees.

530. There are no legal or regulatory requirements which impede the implementation of internal controls and procedures to ensure compliance with AML/CFT requirements, including information sharing between group entities.

Overall conclusions on IO.4

531. Understanding of risk and the application of AML/CFT preventive measures are now generally good in the banking and TCSP sectors – weighted as the two most important sectors. However, this was not the position throughout the whole period under review, with improvements noted particularly after supervisory measures were strengthened in 2019. Before

that, weaknesses were observed regarding business and customer risk assessments and in establishing and corroborating of SoW and SoF in both sectors. These must necessarily influence the rating, notwithstanding many of the positive developments summarised in this chapter.

532. Moreover, the level of suspicious activity reporting, whilst increasing, is still considered to be low, taking account of residual inherent risks, particularly amongst TCSPs, some of which have never made a SAR/STR. The understanding of typologies and red flags also needs to be improved in some smaller non-bank FIs and DNFPBs.

533. The effectiveness of measures implemented by the VASP sector (weighted as highly important) particularly customer profiling, is hindered by an extraordinarily high number of legacy customers without full CDD at one large entity and delayed implementation of the "travel rule" (partly due to the absence of global implementation).

534. As such, taking into account all the above, the evaluation team believes that IO.4 is achieved to some extent and major improvements are needed.

535. Liechtenstein has achieved a **moderate level of effectiveness for IO.4**.

6. SUPERVISION

6.1. Key Findings and Recommended Actions

Key Findings

Immediate Outcome 3

a) The FMA has substantially revised its operations and priorities in order to apply more comprehensive risk-based supervision and more dissuasive sanctions and remediation measures. The FMA and its staff have demonstrated commitment to these changes.

b) Controls implemented by supervisors, including those applied on an ongoing basis, are effective at preventing criminals from holding or being the BO of a significant interest or holding a management function. These controls have successfully picked up a small number of cases of criminal involvement at pre- and post-licensing stages.

c) Positive steps have been taken by the FMA to improve its knowledge of ML/FT risks at national level, across all supervised sectors, and at institutional level. This includes introduction of a specific supervisory risk model at the FMA. Accordingly, the FMA is considered to have a good understanding of risk. Risk assessment by the Chamber of Lawyers is comparatively rudimentary but given the risk and size of the regulated sector, this is not a major concern.

d) The FMA supervisory approach has been subject to a significant overhaul during the review period (2019). In particular: (i) greater use is now made of FMA inspections to conduct reviews of compliance with AML/CFT requirements; and (ii) there is now much greater FMA input into, and oversight of, commissioned inspections, which add an additional supervisory baseline, and which are now more uniform and focussed on higher risk themes that are set by the FMA. Supervision by the Chamber of Lawyers is comparatively rudimentary but given the risk and size of the regulated sector, this is not a major concern.

e) Targeted supervision of compliance with TFS was introduced in 2020 following clarification of supervisory responsibilities. So far, not all persons subject to the DDA have been supervised under this new regime.

f) Direct FMA supervisory activity of entities that it assesses as presenting a high-risk or medium-high risk (predominantly TCSPs and investment funds) is not sufficient. The AT does not consider that one visit to a high-risk entity by the FMA every three years or to a medium-high risk entity every five years is sufficient, even considering the use of supporting commissioned inspections. Resource constraints are a concern. The FMA is insufficiently equipped to deal with high risk and medium-high risk TCSPs and has only been able to perform a marginal number of random checks on medium or medium-low risk institutions in line with its targets.

g) Since 2019, there has been an increasing move towards the use of focussed and thematic inspections. Whilst the AT welcomes the focus on identified risk themes, there remains a need also for some more general supervisory activity to test compliance with the full range of preventive measures at all levels of risk.

h) There has been a notable increase in the imposition of monetary fines since 2019. However, it is not possible to conclude that effective, proportionate, or dissuasive sanctions have been applied by the FMA. Overall, the FMA continues to mostly use remedial supervisory measures to deal with breaches and the number and level of monetary fines imposed during the period under review has been low. In particular, enforcement action against the TCSP sector is less than expected by AT.

i) Supervisors have not clearly demonstrated that their actions have had an effect on compliance, though analysis under Chapter 5 (IO.4) supports the FMA's view that, in general, compliance with AML/CFT obligations has improved as a result of strengthened supervisory measures since 2019.

j) Supervisors promote a clear understanding of AML/CFT obligations and risks.

Recommended Actions

Immediate Outcome 3

a) The FMA should review its targets for the frequency of supervisory activity of entities that it assesses as presenting a high-risk or medium-high risk (predominantly TCSPs and funds). When doing so, it should also consider the use of offsite supervision, e.g., regular desk-based review of business risk assessments, and policies and procedures, to ensure that a full range of AML/CFT obligations continues to be adequately assessed across all sectors.

b) Liechtenstein should increase the number of staff that are available to the FMA to deal with high risk and medium-high risk TCSPs and investment funds and conduct more frequent random reviews of other risk categories.

c) The FMA should make more extensive use of monetary fines, particularly in those sectors identified as presenting a higher risk, in addition to requiring remediation of shortcomings.

d) The FMA should proceed with planned supervisory colleges for banks in 2022 - in line with the relevant Guidelines of the European Supervisory Authorities.

e) The FMA should consider making regular and structured use of suspicious reporting data in its risk modelling in order to attach a higher risk rating to reporting outliers.

f) The FMA should publish the results of its annual round of directly undertaken and commissioned inspections in order to promote a clear understanding of AML/CFT obligations and continue to improve behaviour in the private sector. It should also continue to develop a mechanism to clearly demonstrate the impact of supervision on industry compliance with AML/CFT requirements.

g) FMA supervision should continue to cover compliance with TFS, including screening of existing customers where there are changes to sanctions lists and freezing of assets where necessary. Supervisors should conduct further outreach on TFS – particularly where there is less developed understanding. Outreach should cover compliance with obligations under the TF-related TFS regime, including newly developed guidance, reporting, and scope of persons subject to TFS.

536. The relevant IO considered and assessed in this chapter is IO.3. The Recommendations relevant for the assessment of effectiveness under this section are R.14, 15, 26-28, 34, 35 and elements of R.1 and 40.

6.2. Immediate Outcome 3 (Supervision)

537. The provision of financial services in Liechtenstein is subject to a licencing requirement, with the FMA being the competent authority for granting, amending, and withdrawing licences. The FMA's licensing responsibilities extend also to TCSPs and VASPs. Lawyers are licensed by the Chamber of Lawyers. Other types of DNFBPs, except TCSPs, are licensed by the Office of Economic Affairs. In terms of supervision, all supervision for AML/CFT purposes is conducted by the FMA, with the exception of lawyers, which is conducted by the Chamber of Lawyers. Numbers of FIs, DNFBPs and VASPs licenced or registered on 30 September 2021 are set out in a table in Chapter 1.

538. The following activities which are covered by the FATF definition of FI are not subject to supervision for AML/CFT purposes by the FMA: (i) lending (own funds only); (ii) financial leasing; and (iii) issuing and managing paper-based means of payment. Provisions in respect of legal and accountancy services do not apply to preparing for or carrying out transactions for clients with respect to the creation, operation or management of legal persons or arrangements. However, in practice, these activities are covered by supervision of TCSPs. As explained under Chapter 1, lawyers providing services related to forming and managing legal persons and legal arrangements do so under the umbrella of a TCSP engaged in establishing legal persons or trusts. TCSPs are also licensed to provide tax advice, and so the extent to which external accountants may be needed to provide input with respect to the creation, operation or management of legal persons or arrangements will be limited. Accordingly, gaps in respect of legal and accountancy services are also considered only minor. There is no general regulation or supervision of transfers of VAs which is called for by the FATF Recommendations. Instead, the FMA supervises persons that provide such a service.

539. The figures given in Chapter 1 for TCSPs refer to active TCSPs, under whose umbrella individual licence holders (trustees, trust companies and qualified members/Art. 180a persons) operate. The FMA conducts consolidated AML/CFT inspections in which these individual licensees are jointly inspected on the basis of their legal/economic links with an active TCSP. The number of individual licence holders was as follows: 2016: 619; 2017: 617; 2018: 638; 2019: 665; 2020: 668; and 2021: 649.

540. Whereas fund managers are licensed and supervised for prudential purposes, they are not subject to the DDA or supervision for AML/CFT purposes (except in respect of individual portfolio management). Instead, underlying investment funds are licenced and subject to supervision for AML/CFT purposes. However, there is a very small number of foreign investment funds (four out of more than 600) which are solely administered in Liechtenstein, that have not been supervised for compliance with the DDA by the FMA.

541. The FMA is not responsible for the supervision of business conducted remotely in Liechtenstein by EEA FIs or Swiss insurance undertaking and intermediaries operating with the scope of freedom to provide services. Under EEA arrangements and bilateral agreement with the Swiss, supervision here is the responsibility of the home supervisor in the EEA or Switzerland. In both cases, a notification from the home country authority is required before business can be conducted remotely in Liechtenstein from abroad and the FMA has a regular exchange of

information, including use of AML/CFT colleges and ad-hoc exchanges, if there are indications of non- or poor compliance with European standards.

542. The FMA has substantially revised its operations and priorities in order to apply more comprehensive risk-based supervision and more dissuasive sanctions and remediation measures. The FMA and its staff have demonstrated commitment to these changes.

543. The FMA is established by the FMA Act with its own legal personality. It is independent from the Government and operates as an autonomous institution. Until 2018, AML/CFT supervision was an integrated part of prudential supervision. Since 2019, AML/CFT supervision has become the responsibility of the newly created AML/CFT and DNFBP Division, comprising of two separate sections: (i) the AML/CFT Section (responsible for supervision of all persons subject to the DDA); and (ii) the DNFBP Section (responsible for prudential supervision of DNFBPs and AML/CFT enforcement of all persons subject to the DDA). The AML/CFT section is further divided into two separate teams: (i) the FMA Inspection Team, which is responsible for conducting AML/CFT inspections (eVOKs) and consists of seven staff; and (ii) the Commissioned Inspections and Policy Team, which is responsible for commissioned AML/CFT inspections (bVOKs), the FMA's risk assessment process, policy development and issuing guidance, and consists of four staff.

544. In 2020, average staffing was 112 individuals, of which 16.5 staff are in the AML/CFT and DNFBP Division. This includes: (i) 7 FTE for FMA inspections (eVOKs); (ii) 2.5 FTE for commissioned inspections (bVOKs); (iii) 2.5 FTE for policy work; and (iv) 4.5 FTE enforcement staff. Based on these numbers, and taking account of work undertaken by commissioned auditors, it is not clear that the FMA has sufficient resources to undertake adequate risk-based AML/CFT supervision, taking account of the size, complexity, and risk profile of Liechtenstein's financial, DNFBP and VASPs sectors (specifically 222 individual high and medium-high FIs/DNFBPs).

545. The Chamber of Lawyers is the supervisory authority for all lawyers in Liechtenstein, including, since 2017, AML/CFT supervision of those lawyers subject to DDA obligations. It is operationally independent, with some limited oversight by Government. However, the Government's role is limited to reviewing the legality of the administrative management of the Chamber, and no quality control or comparative analysis is undertaken with regard to the Chamber's supervisory function or activities. This is not a material deficiency in the context of the Liechtenstein regime as a whole.

546. Inspections of the legal sector (which is small in size) are carried out by members of the Chamber's DDA Supervisory Committee, which comprises of five practicing lawyers, three of which are subject to the DDA themselves. Members of the DDA Supervisory Committee are nominated and agreed by the Chamber on an annual basis. Any potential conflicts of interest are managed by way of spreading the workload amongst the five members of the Committee as appropriate, so that no lawyer inspects his or her own law firm or a direct colleague. The AT has some concerns as to the independence of the DDA Supervisory Committee, in light of the small community of supervised lawyers in Liechtenstein.

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

547. Controls implemented by supervisors, including those applied on an ongoing basis, are effective at preventing criminals and their associates from holding or being the BO of an interest

or holding a managing function. There have been examples where criminality has been detected by the FMA.

FMA – FIs, TCSPs and VASPs

548. Responsibility for licensing is spread across four separate divisions within the FMA, each being responsible for licencing their respective sector: namely the Banking Division, the Insurance and Pension Funds Division, the Securities and Markets Division, and the AML/CFT and DNFBP Division. The Executive Office (Regulatory Laboratory/Financial Innovation Group) is responsible for the registration of VASPs. Time limits set for a decision to be taken on a licence/registration application vary across the different divisions, being between one and six months from receipt of all information necessary to support the licence application.

Table 6.1: FMA licence/registration applications by type of applicant (2015 to 2020)

Type of Entity	Number of applications received	Number of licences/registrations approved	Number of licences/registrations refused[19]
Banks, investments firms, E-money institutions	13	6	3
Payment institutions	-	-	-
Fund management companies (individual portfolio management)	21	19	4
Investment funds	299	294	-
Asset managers	47	27	15
Life insurance undertakings	4	-	3
Life insurance intermediaries	29	13	3
TCSPs	134	124	6
VASPs	20	8	2
Total	567	491	36

549. Of the total number of licences refused (36), the FMA has refused: (i) five applications where fit and proper requirements for shareholders were not met; and (ii) ten cases where fit and proper requirements were not met for members of the governing body. Four of these refusals related to criminality issues (two in the banking sector, one in the securities and markets sector and one in the insurance sector).

550. As part of their application for a licence or registration, applicants must submit the following documents: (i) due diligence concept; (ii) process diagrams; (iii) internal instructions; (iv) due diligence concept checklist; (v) statement on the due diligence "concept" by an appropriately qualified person; (vi) business model; (vii) programmes, including policies, controls, and procedures (including group-wide policies); and (viii) in the case of VASPs, compliance tools.

551. All these materials are reviewed by FMA staff in the relevant division in line with internal policies, and this review focuses primarily on whether the applicant is aware of their AML/CFT obligations and ascertaining whether the applicant's policies and procedures align with legal requirements. A more detailed examination of the applicant is then conducted after licencing, as

[19] Differences in numbers occur where either: (i) the date of submission or date of approval/rejection of an application falls outside the relevant time period; or (ii) the application is withdrawn voluntarily, i.e., without refusal by the FMA.

part of an onsite supervisory inspection (normally within 12 months of issuing the licence or registration).

552. In one notable example, the licensing process identified: (i) ongoing criminal investigations associated with an applicant; and (ii) deficiencies in the "AML concept" (application of CDD). Recognising this, conditions were attached to the licence to enable the FMA to review/revise its licencing decision once the outcome of investigations and a remediation programme were known.

Fit and proper testing of significant holdings and senior management

553. Following licensing or registration, FIs, TCSPs and VASPs are required to obtain the written consent of the FMA: (i) to amend an existing licence; (ii) to appoint a person to the governing body (including but not limited to directors); and (iii) to approve a subsequent change in shareholding. There are powers that allow connections to criminals to be considered. The requirements are covered in detail under c.26.3.

554. For natural persons, the fit and proper test applied by the FMA involves the mandatory submission of the following: (i) valid official photo identity document; (ii) curriculum vitae; (iii) current extract from the criminal register; (iv) confirmation of solvency; (v) current statement concerning good repute (fit and proper form including enclosures and declarations); and (vi) and evidence of professional qualifications (where relevant).

555. In addition, FMA staff utilise open sources, external commercial databases, and internal intelligence to check the background of applicants. There is also an entire screening of databases on a weekly basis. Additionally, the FMA interviews individuals by way of a risk-based approach, where there are doubts about suitability e.g., one case where there was speculation about connection to criminal activity.

556. Many of the applications received in respect of shareholders and members of the governing body come from persons with residence or nationality outside the country (given that many working in the financial sector live in neighbouring countries). Where an applicant has lived or worked abroad or is a foreign national, checks are extended to all countries in which the applicant has had a place of residence or worked in the past ten years or has nationality. Information received from abroad has been determinative in some decisions.

557. In order to cover this group of individuals, the FMA liaises with its foreign counterparts, as set out in the table below. Overall, the AT considers that the number of requests appears low, considering the extent to which individuals involved in the Liechtenstein financial sector come from foreign countries, including for TCSPs and investment funds where no requests have been made. The authorities have explained that it is not usual for professionals working in the TCSP sector to have worked outside that sector or in other countries, and so there have been no opportunities to consult with foreign counterparts. While there have been consultations in relation to fund management companies administering investment funds, it is a concern that no additional requests have been made in respect of directors of corporate investment funds themselves.

Table 6.2: Outgoing consultations with foreign counterparts (fit and proper checks)

Type of Entity	2015	2016	2017	2018	2019	2020	Total	Hits[20]
Banks, investments firms, E-money institutions	-	5	9	11	10	12	47	8
Life insurance undertakings	4	7	8	10	11	2	42	7
Life insurance intermediaries	-	-	-	-	-	-	-	-
Fund management companies and asset managers,	2	19	4	8	15	9	57	3
Investment funds[21]	-	-	1	-	2	-	3	2
TCSPs	-	-	-	-	-	-	-	-
VASPs[22]	N/A	N/A	N/A	N/A	N/A	1	1	-
Total	**6**	**31**	**22**	**29**	**38**	**24**	**150**	**20**

558. Changes in the composition of governing bodies cannot be entered in the commercial register held in the Commercial Register Division without the prior approval of the FMA, ensuring that such changes are checked in advance by the FMA. The number of objections to applications for approval of new shareholders (and BOs) and new members of governing bodies post licensing are low: eight during the period from 2015 to 2020. Two of these directly related to criminality - both within the banking sector (one member of a governing body and one relating to a shareholder).

559. Natural persons who have been approved are subject to continual monitoring. The FMA uses various instruments such as media monitoring, and onsite and offsite inspections to make sure that shareholders (and BOs thereof) and members of governing bodies fulfil fit and proper requirements on a permanent basis. For example, several media reports were published about the good standing of an indirect shareholder of a bank, which led to a full review of that individual. Moreover, the FMA picked up a complaint filed abroad by a foreign supervisor against various shareholders of companies connected to a licensed insurance undertaking in Liechtenstein within two days of that filing. Shareholders of that undertaking were under the control of a criminal organisation. There were 49 cases between 2015 and 2020 where the FMA had concerns over propriety post-licensing/registration. These can be classified as follows: banking sector - 26 cases (including 13 "criminality issues"[23]; securities and markets sector - 13 cases (including four

[20] Hits in this table represent the number of occasions a foreign consultation has identified indicators of criminality, irrespective of the indicators' quality (i.e., both "hard" hits and "soft" hits.

[21] Investment funds are established in corporate form (SICAV), in contractual form or in the form of a trust ("collective trusteeship"). The investment fund is typically administered by an external fund management company, although SICAVs also have directors themselves who may exercise control.

[22] Licensing commenced in 2021.

[23] 11 of these cases related to a single bank, where multiple proceedings were initiated against a number of shareholders and members of the governing body.

"criminality issues"); and insurance sector - ten cases (including four "criminality issues" and three mixed criminality/regulatory issues).

Chamber of Lawyers - lawyers

560. Fitness and properness checks on lawyers by the Chamber of Lawyers are generally sufficient.

561. The Chamber is responsible for the admission of lawyers in Liechtenstein and associated fitness and propriety checks. Only EEA citizens may become lawyers in Liechtenstein. Organisationally, lawyers may associate in the form of partnerships or companies, but it is the individual lawyer that is licenced (not the firm) and who remains responsible for carrying out his or her activities (including complying with AML/CFT requirements). Only lawyers entered into the Liechtenstein register of lawyers can be partners in a Liechtenstein law firm.

Table 6.3: Applications for admissions

Admissions	2016	2017	2018	2019
Lawyers	12	12	18	10
Resident European lawyers	7	3	10	9
Total	19	15	28	19

562. During admission proceedings for lawyers, an applicant must submit: (i) an up-to-date curriculum vitae; (ii) an up-to-date proof of solvency; (iii) a personal declaration concerning insolvency proceedings; (iv) a copy of a valid passport or valid identity card; (v) an extract from the Register of Convictions (including foreign equivalent); and (vi) a personal declaration concerning any pending criminal and/or administrative proceedings. Open sources and external commercial databases are used at the time of licensing.

563. No application was formally dismissed during the reporting period. Whilst several applications led to the Chamber of Lawyers seeking talks with the applicant, none related to identified criminality.

564. Following admittance, disciplinary proceedings against a lawyer will automatically follow any conviction for a criminal offence. Whilst the Chamber of Lawyers takes no proactive measures to monitor criminal proceedings in respect of its membership, the Liechtenstein court immediately informs the Chamber in such circumstances. Similar arrangements are in place with Austria, which accounts for the majority of resident European lawyers.

Office of Economic Affairs – accountants, estate agents and DPMS

565. The Office of Economic Affairs is responsible for the licencing of all commercial entities (including accountants, estate agents and goods traders) under the Business Act. Natural and legal persons are excluded from carrying out these activities if (amongst other things) they have been convicted of a specified crime (including any for imprisonment exceeding three month) or been subject to bankruptcy proceedings or equivalent.

566. Checks are generally sufficient, given the risk context of these sectors. The Office of Economic Affairs undertakes checks on the BOs of DNFBPs, in addition to the managing director and operations manager of applicants (who must be resident in Liechtenstein, the EEA or Switzerland). Checks undertaken always include obtaining a current excerpt from the criminal register of the country in which the individual is resident (not older than 3 months). The Office also liaises with the FMA and Office of Justice. There are no ongoing checks to ensure that changes

are reported or to pick up changes in circumstances. Where there are changes in BO, the Office of Economic Affairs relies on notification from the FMA (supervisor).

Office of Economic Affairs - casinos

567. Fitness and properness checks on casinos are generally sufficient and operate effectively. So far, only five casinos have been licenced – all of which have European parent companies.

568. The Office of Economic Affairs issues licences for casinos under the Gambling Act and checks the fitness and propriety of shareholders (including BOs), members of the board of directors, key function holders and main business partners - taking account of criminal, tax, financial and wealth-related information. Directors and key function holders submit a dossier including an extract from the criminal register as well as an extract from the Garnishment Register (solvency) (original and not older than three months) and confirm also that there are no outstanding proceedings.

569. In respect of the applicant itself, detailed checks are completed on the SoF to set up a casino. In order to do so, transactions for the past five years are reviewed.

Table 6.4: Number of casino applications received by the Office of Economic Affairs

Licence Applications	2017	2018	2019	2020	TOTAL
Received	2	-	3	1	6
Approved	2	-	2	1	5
Withdrawn	-	-	-	1	1
Refused	-	-	-	-	-

6.2.2. Supervisors' understanding and identification of ML/TF risks

FMA

570. Positive steps have been taken to improve knowledge of ML/FT risks at national level, across all supervised sectors, and at institution level. This includes involvement in the conduct of the various national risk assessments as well as the introduction of a specific supervisory risk model at the FMA. Accordingly, the FMA is considered to have a good understanding of risk.

571. The following inherent and residual ML risks were determined in NRA II.

Table 6.5: Sectoral inherent and residual ML risks

Sector	Inherent Risk	Residual Risk
Banks	High	Medium-high
TCSPs	High	Medium-high
Insurance undertakings	Medium-high	Medium
Asset managers	Medium-high	Medium
Investment funds	Medium-high	Medium
Insurance intermediaries	Medium	Medium
Casinos	Medium	Medium-low
Other DNFBPs	Medium-low	Low

572. In 2017, the FMA introduced an extensive data collection exercise by way of an annual questionnaire for all supervised persons that collects both qualitative and quantitative information. The questionnaire includes questions on types of services and products offered, numbers and types of customers, delivery channels, and geographical exposure and is tailored to individual sectors. Information is reported through an electronic reporting platform (AML reporting).

573. The first questionnaires were submitted in 2018, based on data for 2017. This means that there have already been four full reporting cycles (three cycles for banks). The system is reviewed regularly, and additional reporting factors were added following the conclusion of NRA II - in order to improve the availability of information in identified risk areas. Additional data points are also added annually as risk understanding increases in granularity. Data collected includes specific TF risk factors/indicators and provides a strong basis for the FMA to understand and identify ML/FT residual risks.

574. The FMA's internal risk model (known as the "AML-RAS") applies sectoral and entity weightings to the data collected to develop sectoral and entity risk profiles. Weightings used and outputs are subject to review and sense-checks. In addition, the following are taken into account in the risk assessments for individual entities: (i) sectoral risk; (ii) information from FMA and commissioned inspections; and (iii) enforcement activities. Although suspicion reporting behaviour is considered in the context of individual inspections, there is currently no methodical use of suspicious reporting data in risk modelling to attach a higher risk to reporting outliers (either sectors or individual supervised persons).

575. The FMA has not prepared individual risk profiles for some sectors that have been assessed as presenting a low risk (DPMS, real estate agents, tax advisers, external accountants, and exchange offices).

576. Individual entities have been risk-rated by the FMA as high, medium-high, medium, and medium-low. The table below summarises the risk ratings calculated for all FIs, DNFBPs and VASPs (except lawyers). An annual report is made to the board on risk weightings.

Table 6.6: Risk ratings of subject persons - September 2021

Industry Sector	Total Population	High Residual Risk	Medium/High Residual Risk	Medium Residual Risk	Medium/Low Residual Risk
Banks	12	2	6	3	1
Payment institutions - agent	1	-	-	1	-
E-money Institutions	3	-	-	2	1
Fund management companies	6	-	1	2	3
Investment funds	676	2	64	412	198
Asset managers	101	3	22	50	26
Life insurance undertakings	18	1	4	8	5
Life insurance intermediaries	21	-	3	7	11

TCSPs	188	39	69	49	31
Casinos	5	1	1	2	1
Other DNFBPs	21	-	-	-	21
VASPs	10	3	1	-	6
Total	1,062	51	171	536	304

577. Some banks operate as groups through foreign branches and subsidiaries. The risk ratings for such banks take into account the additional risks that may be presented by operating in foreign markets, being adjusted manually (a group risk "premium"). Additional information is collected through a supplementary questionnaire, first used in 2019 but which has been updated since. The questionnaire collects both quantitative and qualitative information. There are also ten TCSPs with subsidiaries or branches abroad, mainly located in the BVI, China, Hong Kong, Panama, Singapore, and Switzerland. These are not considered material by the authorities and so no supplementary measures have been applied. This point is considered further under Chapter 2 (IO.1).

578. All data collected via AML reporting is analysed using a display programme. This allows data to be displayed using various dashboards at both individual and sectoral level. This facilitates the comparison of data on a sector specific and cross-sectoral basis.

579. There is close cooperation between the AML/CFT Section (responsible for supervision) and prudential departments. Every two weeks, chief supervisors in all areas exchange information about current risks and cases and, on an annual basis, AML/CFT and prudential analysts discuss mutual risk classifications.

580. In addition to the FMA's membership of the PROTEGE WG, it hosts a meeting every two months with the FIU, OPP, Fiscal Authority and STIFA. As part of the exchange of information, current supervision cases are discussed. This is a key element that influences risk-based supervision. For example, the FMA can adjust or add further risk factors.

Chamber of Lawyers

581. Risk assessment by the Chamber of Lawyers is comparatively rudimentary but, given the risk and size of the regulated sector, is not a major concern.

582. The Chamber of Lawyers was involved in preparing NRA I. This concluded that the residual ML risk in the legal sector was medium-low.

583. All lawyers submit a return to the Chamber whenever they undertake an engagement that is subject to the DDA. The Chamber then uses this information to assess the relative risk of lawyers, based primarily on the number of engagements. Generally, lawyers have no more than five such engagements annually. Lawyers may be risk rated as high, medium-high, medium, and medium-low risk.

6.2.3. Risk-based supervision of compliance with AML/CFT requirements

FMA

584. Positive action has been taken by the FMA to enhanced risk-based supervision. However, FMA onsite supervisory activity of entities that it assesses as presenting a high-risk or medium-high risk (predominantly TCSPs and funds) is not considered to be sufficient and resource

constraints are a concern. There has been a clear supervisory focus on the particular risks that were identified by the NRA.

585. The FMA supervisory approach has been subject to a significant overhaul during the review period (2019). In particular: (i) greater use is now made of FMA inspections (eVOKs) to review compliance with AML/CFT requirements – in order to develop closer insight into the higher risk operations of supervised entities; and (ii) there is now much greater FMA input into, and oversight of, commissioned inspections (bVOKs), which add an additional supervisory baseline, and which are now more uniform and focussed on higher risk themes that are set by the FMA. These developments are welcomed.

586. The FMA has expressed a desire to move toward a 50:50 split between FMA and commissioned inspections. Despite the increased number of FMA inspections, the majority of supervision of the most important and highest risk entities is still undertaken by commissioned auditors.

587. The FMA's supervisory approach – in place since 2019 - provides that institutions assessed by the FMA as being in the high and medium-high risk categories (**individual risk** ratings based on the FMA's internal risk model) should be directly monitored by the FMA, with a focussed onsite inspection at least every three and five years respectively. The FMA will conduct random onsite inspections for other risk categories. In the case of commissioned inspections, the frequency of thematic inspections is based on **sectoral risk.** At least two inspectors take part in FMA and commissioned inspections, spending one to two weeks onsite, depending on size and the extent of sampling undertaken. Under the supervisory approach, full-scope inspections should be conducted only for new market entrants.

Table 6.7: Targeted frequency of planned FMA and commissioned inspections

Risk	FMA inspections (eVOK) – frequency based on individual risk assessments	Commissioned inspections (bVOK) – frequency based on sectoral risk assessments
High	Every 3 years	Annual
Medium-high	Every 5 years	Banks, TCSPs, VASPs - every 3 to 4 years
Medium	Random	Insurance, asset managers, investment funds - every 5 years
Medium-low	Random	Others (incl. Casinos[24], accountants, DPMS)- not used

588. The AT does not consider that one visit to a high-risk entity by the FMA every three years or to a medium–high entity every five years is sufficient, even considering the use of supporting commissioned inspections (where entities are assessed on at least a three to four year rolling basis) as these are not specifically designed to supplement the coverage of FMA inspections. Further, all planned inspections since 2019 have been focussed or thematic (except for newly licensed entities) rather than full scope, and so even when FMA and commissioned inspections

[24] Casinos have been subject to annual (eVOK) inspections, due to the industry being new. Random checks will be conducted in the future.

are combined, they do not consider whether entities are meeting all their AML/CFT requirements (a point that is considered further later).

589. Whilst it is still early days for this new approach, resource constraints mean that the FMA has not been able to meet its own frequency targets for onsite inspections. Whilst institutions that it has assessed as presenting a high or medium-high risk (individual risk assessments) have been examined directly by the FMA (predominantly TCSPs and investment funds), the overall number of visits undertaken has been well under the above targets[25], and it has only been able to perform a marginal number of random checks on medium or medium-low risk institutions.

590. On a more positive note, targets have been met for regular FMA inspections of banks and commissioned inspections, except, in the case of the latter, for investment funds. Indeed, in the case of banks, all have been inspected by auditors on an annual basis throughout the period under review, and a number of ad hoc reviews also undertaken.

591. Overall, resource constraints are a concern. In particular, they mean that: (i) the supervisor is insufficiently equipped to deal with high risk and medium-high risk TCSPs and investment funds; and (ii) it may not be possible for the FMA to conduct a sufficient number of random reviews, checking compliance with AML/CFT obligations in lower risk sectors. It is important that more supervisory resources are directed to these areas, particularly given additional supervisory responsibilities recently placed on the FMA in respect of VASPs and casinos, the former in particular being resource intensive.

Table 6.8: Actual scheduled and ad hoc onsite activity – FMA and commissioned inspections (excluding follow-up inspections)

Number of entities and inspections	2016	2017	2018	2019	2020	2021 (Sep)
Banks	**15**	**15**	**14**	**14**	**14**	**12**
Full scope (eVOK)	-	-	-	-	-	-
Focused (eVOK)	4	3 (+2 ad hoc)	2 (+1 ad hoc)	2 (+2 ad hoc)	3 (+3 ad hoc)	5
Full scope (bVOK)	15	15	14	14	-	-
Thematic (bVOK)	-	-	-	-	14	12
Investment firms	**1**	**1**	**1**	**-**	**-**	**-**
Full scope (eVOK)	-	-	-	-	-	-
Focused (eVOK)	-	-	-	-	-	-
Full scope (bVOK)	-	1	1	-	-	-
Thematic (bVOK)	-	-	-	-	-	-
Payment institutions - agents	**1**	**2**	**1**	**1**	**1**	**1**
Full scope (eVOK)	-	-	-	-	-	1
Focused (eVOK)	-	-	-	-	-	-
Full scope (bVOK)	-	-	-	-	-	-

[25] At September 2021 there were 51 high risk entities and 171 medium-high risk entities. In line with the approach set by the FMA, 17 high risk entities should be inspected each year and 34 medium-high risk entities – in total 51. In 2019 there were 25 regular/cyclical inspections and in 2020 there were 34 regular inspections.

Thematic (bVOK)	-	-	-	-	-	-
E-money institution	**2**	**2**	**3**	**5**	**4**	**3**
Full scope (eVOK)	-	-	-	-	-	-
Focused (eVOK)	1	-	-	-	2	-
Full scope (bVOK)	1	2	2	1	-	-
Thematic (bVOK)	-	-	-	-	-	-
Fund management companies (individual portfolio management)	**2**	**5**	**7**	**7**	**6**	**6**
Full scope (eVOK)	-	-	-	1	1	1
Focused (eVOK)	1	-	-	-	-	-
Full scope (bVOK)	1	5	2	-	-	-
Thematic (bVOK)	-	-	-	-	2	2
Investment funds	**N/A**	**-**	**684**	**613**	**643**	**676**
Full scope (eVOK)	-	-	-	4	6	2
Focused (eVOK)	-	-	-	- (+1 ad hoc)	-	-
Full scope (bVOK)	-	-	15	120	-	-
Thematic (bVOK)	-	-	-	-	21	21
Asset managers	**116**	**109**	**109**	**104**	**102**	**101**
Full scope (eVOK)	-	-	-	7	2	1
Focused (eVOK)	5	-	-	- (+1 ad hoc)	-	-
Full scope (bVOK)	116	109	22	18	-	-
Thematic (bVOK)	-	-	-	-	29	29
Life insurance undertakings	**21**	**21**	**21**	**21**	**19**	**18**
Full scope (eVOK)	-	-	-	-	-	-
Focused (eVOK)	3	4 (+1 ad hoc)	5 (+1 ad hoc)	2	2	3
Full scope (bVOK)	20	21	20	18	-	-
Thematic (bVOK)	-	-	-	-	1	5
Life insurance intermediaries	**51**	**43**	**30**	**31**	**30**	**21**
Full scope (eVOK)	-	-	-	-	-	-
Focused (eVOK)	4	3	-	-	1	2
Full scope (bVOK)	12	6	7	5	-	-
Thematic (bVOK)	-	-	-	-	7	4
TCSPs (licences holders) [26]	**189 (619)**	**188 (617)**	**184 (638)**	**188 (665)**	**185 (668)**	**188 (649)**
Full scope (eVOK)	-	-	-	7	11	17

[26] The lower figure refers to active TCSPs under whose umbrella individual licence holders (trustees, trust companies and Art. 180a persons) operate. The higher number is for individual licence holders. The FMA conducts consolidated AML/CFT inspections in which individual licensees are jointly inspected on the basis of their legal/economic links, so that each of the TCSP inspections in the table comprises an average of 3 to 4 individual TCSP licence holders.

Focused (eVOK)	14 (+5 ad hoc)	9 (+2 ad hoc)	7 (+7 ad hoc)	- (+4 ad hoc)	-	1 (+1 ad hoc)
Full scope (bVOK)	53	68	55	58	-	-
Thematic (bVOK)	-	-	-	-	40	33
Tax consultancy	**N/A**	**-**	**-**	**1**	**1**	**1**
Full scope (eVOK)	-	-	-	-	-	-
Focused (eVOK)	-	-	-	-	-	-
Full scope (bVOK)	-	-	-	-	-	-
Thematic (bVOK)	-	-	-	-	-	-
Accountants	**N/A**	**-**	**6**	**8**	**7**	**7**
Full scope (eVOK)	-	-	-	-	-	-
Focused (eVOK)	-	-	-	-	-	-
Full scope (bVOK)	-	-	-	-	-	-
Thematic (bVOK)	-	-	-	-	-	-
Estate agents	**-**	**7**	**3**	**4**	**6**	**6**
Full scope (eVOK)	-	-	-	-	-	-
Focused (eVOK)	-	-	-	-	-	-
Full scope (bVOK)	-	-	-	-	-	-
Thematic (bVOK)	-	-	-	-	-	-
High value goods dealers	**7**	**3**	**3**	**4**	**6**	**7**
Full scope (eVOK)	-	-	-	-	-	-
Focused (eVOK)	-	-	-	-	1	-
Full scope (bVOK)	-	-	-	-	-	-
Thematic (bVOK)	-	-	-	-	-	-
Casinos	**-**	**2**	**2**	**4**	**5**	**5**
Full scope (eVOK)	-	-	2	-	2	1
Focused (eVOK)	-	-	-	2	-	-
Full scope (bVOK)	-	-	-	-	-	-
Thematic (bVOK)	-	-	-	-	-	-
Crypto exchange/VASPs	**N/A**	**1**	**3**	**3**	**13**	**10**
Full scope (eVOK)	-	-	-	-	3	1
Focused (eVOK)	-	-	-	-	- (+2 ad hoc)	- (+1 ad hoc)
Full scope (bVOK)	-	-	-	-	12	1
Thematic (bVOK)	-	-	-	-	-	-

592. There has been a clear supervisory focus in recent years on the particular risks that have been identified by the NRA. Focused and thematic inspections (both undertaken directly by the FMA and via commissioned auditors) have checked that: (i) business and customer risk assessments are in place; and (ii) CDD measures are applied (in particular that BOs and SoW and SoF are established for politically exposed persons (PEPs) and higher risk customers). Inspections include a risk-based sampling of customer files. For 2021, thematic commissioned inspections of banks covered the implementation of TFS, suspicious activity reporting as well as

BO (postponed from 2020 due to COVID constraints). In addition to the above, FMA inspections have also covered ongoing monitoring and transactions screening, application of group AML/CFT programmes, TF risks, processing of cash transactions, use of shell companies, and other topics identified in the NRA.

593. In line with the supervisory approach explained above, there has been an increasing move towards the use of focussed and thematic inspections for planned and ad-hoc inspections. Whilst the AT welcomes the focus on identified themes, since it allows resources to be directed to areas where risks are greatest, for supervision to be fully effective, there remains a need also for more general supervisory activity to test compliance with the full range of measures set in the DDA/DDO etc by FIs, DNFBPs and VASPs at all levels of risk. This may be done through both offsite and/or onsite supervision.

594. During the period under review, the FMA has conducted visits of group entities in Austria and Luxembourg as well as joint visits with supervisors in Singapore. The FMA has not yet run any supervisory colleges in respect of Liechtenstein-based groups, but such colleges are scheduled for 2022 - in line with Joint Guidelines for the European Supervisory Authorities on cooperation and information exchange.

All inspections

595. Inspection reports are prepared and must be presented to the subject entity within two months of the inspection, although several industry participants commented that reports following FMA inspections often take significantly longer than this to be received.

596. As part of onsite inspections, methodologies supporting IT hardware and software that are used to monitor and screen transactions are reviewed. The FMA does not conduct full IT audits (technical programming of systems, interfaces, etc.) itself, but does make use of relevant experts. In addition, one member of the AML/CFT Section has recently certified as an IT auditor. The FMA is careful to select only commissioned auditors that have necessary IT capabilities, when appropriate.

Commissioned inspections

597. Commissioned inspections are undertaken by specialist auditors, who receive specific AML/CFT training, and training on the assessment methodology to be applied. The entity to be inspected is able to nominate an auditor to perform its inspection, and usually nominates the audit firm that undertakes its financial audits. These nominations are generally accepted by the FMA, although the possibility remains that the FMA may reject the nomination and commission its own choice of auditor. This happens where a nominated auditor is too small or has insufficient experience in AML/CFT matters. Around 20 auditing companies are involved in the process.

598. Following the last MER, the FMA has taken several measures to improve the quality and control over the work of commissioned auditors, including stricter qualification requirements, additional specific training, and mandatory audit work papers. Prior to 2019, audit firms still had some discretion in carrying out inspections, particularly the detailed content of each individual inspection. Since 2019, the FMA has taken more control of the bVOK programme and now specifies the mandatory inspection questions and decides whether an audit finding is a breach of law. The FMA reviews all factual findings drafted by the auditor and makes any necessary decisions as to follow-up action and or sanctions to be applied. During the period, five quality controls were also conducted to review work being done by commissioned auditors.

Offsite supervision

599. Little use is made of offsite supervision tools to support onsite activity. Other than "follow-up inspections" to consider remediation action taken to address deficiencies identified in FMA inspections, most offsite activity is focused on assessment of AML/CFT systems of applicants at the time of licensing and data collection for risk assessment purposes. There is, for instance, no regular desk-based review of business risk assessments, policies and procedures, or any other data or information that might indicate the extent to which FIs, DNFBPs and VASPs are complying with their AML/CFT obligations.

Chamber of Lawyers

600. Supervision by the Chamber of Lawyers is comparatively rudimentary but, given the risk and the size of the regulated sector, this is not a major concern. At least 75% of admitted lawyers do not carry out any activities that are subject to AML/CFT supervision and a significant proportion also hold TCSP licences and are therefore supervised by the FMA. The total population of lawyers subject to AML/CFT supervision by the Chamber is therefore comparatively small; being around 20 lawyers who deal with real estate or escrow accounts.

601. The Chamber of Lawyer's risk-based supervisory strategy calls for an annual inspection of lawyers who are in the highest risk category (high risk), every two years for medium-high, and every three years for medium and medium–low. Currently, no lawyer is in either the high or medium-high risk categories. The medium risk category currently covers seven lawyers, and the medium-low risk category covers 13.

602. In 2018 and 2019, six lawyers from the medium risk class and five lawyers from the medium-low risk class were subject to inspections. Information has not been provided for earlier or later years. Inspections always cover compliance with the DDA/DDO on a full scope basis and thematic or focussed inspections are not used.

Targeted financial sanctions

603. The FMA and Chamber of Lawyers have been designated as competent supervisory authorities for supervising compliance with TF-related TFS since January 2020. Prior to this, only limited actions were applied, including transfer of information by the FMA to the FIU to support a desk-based review of written responses provided by FIs, DNFBPs and VASPs to compliance questionnaires.

604. Since the introduction of targeted TFS supervision, a limited number of onsite inspections have been conducted by the FMA and commissioned auditors and no major issues have been identified so far. As regards the Chamber of Lawyers, it does not conduct targeted TFS supervision, although the presence of screening tools for sanctions lists would be usually checked during its inspections. Given the risk and size of the regulated legal sector this is not a major concern.

6.2.4. Remedial actions and effective, proportionate, and dissuasive sanctions

FMA

605. Overall, the FMA continues to mostly use remedial supervisory measures (informal remediation action plans and orders to restore lawful state of affairs) to deal with breaches. It is surprising that more moderate breaches of the DDA by TCSPs have not been identified which require sanctioning through monetary fines given the risk and levels of compliance observed in

that sector. It has not been possible to apply administrative sanctions to legal persons until very recently. Overall, whilst there has been a notable increase in the imposition of monetary fines since 2019, it is not possible to conclude that effective, proportionate, or dissuasive sanctions have been applied by the FMA.

606. The FMA has a broad range of "supervisory measures" and "administrative sanctions" available in statute to encourage compliance. The former includes warnings, orders to restore the lawful state of affairs, prohibition from taking on new business relationships, and withdrawal of licence, and the latter covers monetary fines. The FMA also sets (informal) remediation action plans.

607. Since 2019, enforcement proceedings have become the responsibility of the DNFBP Section. While this is part of the AML/CFT and DNFBP Division, it is separate from the direct AML/CFT supervision function. This is to ensure a more consistent and independent decision-making process as well as to build up specific expertise on enforcement processes and procedures.

608. Enforcement action generally commences on the recommendation of the AML/CFT Section – as a result of findings from FMA (eVOK) or commissioned (bVOK) inspections. The DNFBP Section reviews the facts and forms a recommendation for sanction or further action which is presented to a regular management meeting which prioritise cases and makes the final decision on any proceedings.

609. Supervisory measures may be imposed directly by the FMA. Prior to 2017, monetary fines were only imposed by the courts. These are now also imposed directly by the FMA, with the ability to impose a monetary fine on legal persons being introduced in 2021. Higher monetary fines may be applied for "substantial, repeated and systematic breaches", terms that are not defined in law. The FMA's enforcement policy and guidance explains that this covers offences that respectively: (i) have a material impact in respect of the concerned obligation and therefore can be described as grievous in the context of an overall assessment; (ii) are repeated more than twice; or (iii) involve a degree of planning or intentional behaviour. Limitations on when a legal person may be fined are explained at c.28.4(c) in the TC Annex.

610. In addition, there are various specific criminal offences (e.g., non-reporting of suspicion) that remain the responsibility of the criminal court. In these cases, the case file and opinion prepared by the DNFBP Section is submitted to the OPP to take forward in the criminal courts[27].

611. In line with the FMA's enforcement policy, minor and moderate breaches are addressed, inter alia, through warnings, agreed (informal) remediation actions plans, and orders to restore the lawful state of affairs. Monetary fines are applied in the case of moderate and serious breaches. Prohibitions on accepting new business, exclusions from management, and licence withdrawal are used only in the case of serious breaches.

612. Any FMA decision in relation to a serious violation of the DDA/DDO must be published. However, if publication of the name of the entity or individual would be disproportionate or likely to jeopardise the stability of the financial markets or ongoing investigations, the FMA may publish

[27] There were nine cases during 2016 to 2021, all relating to banks and TCSPs. All were considered one-off breaches and not linked to systems failures.

its decision anonymously. In practice, the FMA publishes the majority of decisions, even for moderate failings.

Remedial actions

613. The use of remediation action plans (informal measure) and "orders to restore the lawful state of affairs" (formal measure) are used in order to quickly remedy any identified failings in preventative measures. These may be imposed either in addition to, or as an alternative to, other supervisory measures and administrative sanctions. The FMA was unable to provide statistics on how many of its inspections resulted in agreed remediation action plans (informal measure) although a number of case studies were provided. In the case of commissioned inspections, the figure averages around 20%.

614. Deadlines are set for remedial actions to be taken (both in remediation action plans and formal orders). Time periods for completion vary depending on the nature and extent of remediation required and formal orders specifically refer to the possibility of further action (including a monetary fine) should remediation not be completed by the deadline. The FMA monitors implementation of its remediation plans and orders, either by submission of written reports or, where appropriate, by further follow-up inspections. "Follow-up inspections" to check on informal plans and orders were undertaken in approximately 25% of cases identified through an FMA inspection (eVOK), such inspections being offsite. All remediation action plans set through commissioned inspections (bVOK) (referred to as "instructions to restore") are followed-up, typically onsite, with results of the follow up exercise reported to and reviewed by the FMA.

Other supervisory measures and administrative sanctions

615. The following table provides an overview of actions taken during the period under review, including orders to restore the lawful state of affairs (treated as remedial actions).

Table 6.9: Remedial action and sanctions applied

Year	Inspections	Inspections with findings[28]	Inspections leading to remediation plans (auditors only)	Orders to restore (FMA)	Prohibition on new business	Number of fines	Value of fines (CHF)	Criminal complaint[29]
2016	255	32	32	6	-	7	13 350	-
2017	251	34	34	-	-	1	11 800	2
2018	163	31	31	11	-	2	209 000	2
2019	267	53	39	21	-	8	97 000	2
2020	165	66	47	15	1	8	1 034 000[30]	3

[28] Excludes minor findings.

[29] Prior to 2018, CDD failures were dealt with by making a criminal complaint to the court (including one of the two cases in 2017). Otherwise, all criminal complaints relate to failures to report suspicion (one of the few offences that still falls within the competence of the courts). Three relate to banks and six to TCSPs. All cases related to one-off breaches; no systemic issues were detected. The FMA has not across a case where there were indications that the STR/SAR was not submitted on purpose. None of the cases were linked to the amendment to Art. 165 CC (i.e., concerning tax issues and/or shell companies).

[30] Of these fines, CHF 1 million relates to banks and CHF 15 000 to TCSPs.

2021	144	43	26	6	1	26	517 000[31]	-

616. During the period from 2016 to 2021 there were no licence withdrawals or exclusions placed on individuals from holding management positions.

617. Overall, there has been a notable increase in the imposition of monetary fines since 2019, which demonstrates an increasing commitment by the FMA to impose more dissuasive fines for AML/CFT breaches. However, the FMA continues to mostly use remedial supervisory measures (informal remediation action plans and orders to restore lawful state of affairs) to deal with breaches of AML/CFT requirements, and the level of fines is considered by the AT to be generally low for higher risk sectors (banking and TCSPs) which, based on profitability, are likely to have a higher propensity to pay[32]. This low level of fines may be explained by rules set by the FMA Complaints Commission which, in the case of a first offence, has set, as a general rule, a threshold of 10% of the maximum penalty.

618. Given that: (i) NRA II identifies a medium-high residual ML risk for TCSPs; (ii) NRA II highlights common shortcomings amongst TCSPs in the application of CDD and reporting requirements; and (iii) the majority of complaints to the OPP relate to TCSPs, it is surprising that more moderate breaches of the DDA/DDO have not been identified which require sanctioning through monetary fines. This may reflect a relatively low number of FMA inspections undertaken during the period under review (see above). It is also noteworthy that not a single sanction has been applied against an investment fund, though this may reflect the fact that most are not required to apply CDD measures to underlying investors.

619. In cases where serious failures are detected, the FMA has been able to demonstrate taking proportionate and dissuasive action. In 2019, it started a licence withdrawal process against a bank that could not demonstrate compliance with own funds requirements and where shareholders were subject to ongoing criminal proceedings for serious ML. Two cases studies provide evidence in this respect.

Box 13: Bank A - fine and prohibition on new business

The FMA received a self-notification from Bank A based on the results of a post-due diligence investigation mandated by the buyer of the bank. This highlighted repeated violations of the DDA and organisational deficiencies. The FMA issued a decree immediately prohibiting Bank A from taking on new business. In addition, periodic (monthly) reporting on the investigation of the deficiencies was ordered and an action plan was demanded.

At the same time, the FMA conducted an ad hoc onsite inspection of Bank A. In the course of the inspection, it was found that, following the self-notification, the on-boarding process has been adjusted, personnel resources were strengthened, and new appointment made to key positions. On this basis, Bank A was permitted to take on new business again, subject to some restrictions.

[31] Of these fines, CHF 136 000 relates to banks, CHF 145 000 relates to TCSPs, and CHF 131 000 relates to VASPs.

[32] It is noted that the authorities do not routinely collect information on the profitability of DBFBPs, including TCSPs, adding to concerns about proportionality.

Administrative proceedings were initiated for failure to comply with enhanced monitoring obligations and create adequate business profiles in a repeated manner. There were also significant weaknesses in the bank's internal control system. The FMA imposed a fine of CHF 350 000 on Bank A. In determining the fine, its willingness to cooperate was taken into account.

Box 14: TCSP B – fine and criminal complaint

On the basis of a notification from the OPP, the FMA filed a criminal complaint with the Court of Justice against TCSP B on suspicion of failure to file a SAR/STR.

The FMA also initiated administrative proceedings against TCSP C on suspicion of failure to establish the identity of the BO linked to the criminal complaint, failure to create and update the business profile, and failure to monitor the business relationship commensurate to the risk. The FMA issued a fine of CHF 40 000 against TCSP B and also ordered that a lawful state of affairs be restored. When determining the fine, the accumulation of several violations and the repetition of offences were taken into account.

TCSP B lodged a complaint against the FMA's decision which was partially upheld by the Complaints Commission. The fine was reduced to CHF 15 000.

620. Appeals against supervisory measures or administrative sanctions imposed by the FMA can be made to an independent FMA Complaints Commission (whose members are a Court of Appeal judge and high court judges). Appeals over the review period are described as being mainly on technical legal grounds, as FMA enforcement staff have come to terms with application of the relevant laws. The FMA suggest that, more latterly, most decisions of the FMA have been upheld as the understanding of FMA staff and the robustness of the process has improved, although this view is not clearly supported by statistics provided – see below.

621. Several industry participants described having monetary fines reduced on appeal, although statistics provided by the FMA do not indicate this to be a common occurrence. It has been explained that the FMA Complaints Commission gives more weight to mitigating factors than the FMA.

Table 6.11: Appeals to Complaints Commission/results

	2016	2017	2018	2019	2020	2021
Appeals	-	1	-	3	2	-
Confirmed FMA decision	-	1	-	-	-	-
Partial confirmation	-	-	-	2	1	-
FMA decision overturned	-	-	-	1	1	-
Penalty reduced	-	-	-	2: 40k to 15k; 100k to 22k	1: 10k to 5k	-

Chamber of Lawyers

622. The Chamber of Lawyers has not issued any sanctions since the beginning of its jurisdiction on 1 September 2017. Details have not been provided on the application of remedial actions taken.

623. Currently, there is one disciplinary proceeding where suitable provisional measures have been ordered by the Court of Justice and the Chamber has been charged with monitoring a law firm. This relates to an indictment for ML and violation of the requirement of a lawyer (acting as a trustee) to report a suspicion of ML.

6.2.5. Impact of supervisory actions on compliance

624. Supervisors have not clearly demonstrated that their actions have had an effect on compliance.

FMA

625. The FMA has provided a number of sources to demonstrate that its actions have an effect on compliance: (i) summary of findings from FMA inspections on selected (but not all) breaches of AML/CFT obligations for 2019 and 2020 (but not earlier periods); (ii) summary of results of commissioned inspections for 2015 to 2018 and 2020 showing breaches; (iii) detailed summaries of findings from FMA and commissioned inspections; and (iv) a number of cases studies describing the content and the findings of individual inspections. The summary of findings from FMA inspections (item (i)) show mixed results in terms of improvement vs. deterioration of compliance rates and covers too short a time period to enable identification of any trends in this regard. Results from inspections (items (ii) and (iii)), whilst helpful, do not readily identify all cases where there have been improvements in compliance, and analyses (item (ii)) are limited to current and comparative periods.

626. Based on the above, the FMA considers that compliance with AML/CFT requirements has improved over the review period. However, it has not presented a qualitative description of annual inspection findings, setting out trends observed over the period under review though it has already taken some tentative steps in this direction. Accordingly, evidence presented does not allow the AT to draw clear conclusions in terms of improvement vs. deterioration of compliance rates for the full review period or clearly identify overall (long-term) trends.

627. Notwithstanding this, most industry participants supported the FMA's view that compliance with AML/CFT obligations has generally improved, with several referring to recent changes in supervisory approach and increasing enforcement action by the FMA as being drivers for improving standards of compliance – see Chapter 5 (IO.4). In relation to suspicion reporting, statistics in Chapter 5 (IO.4) indicate that the number of reports is generally increasing, particularly for banks and TCSPs in the last two years. Analysis under IO.4 indicates, however, that reporting levels are still considered to be low (particularly in higher risk sectors) and it is less clear whether the *quality* of reporting is improving.

Chamber of Lawyers

628. The Chamber of Lawyers has not provided specific material to demonstrate whether its actions have an effect on compliance.

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

629. The authorities, including the FMA, organise, and participate in, a number of seminars, consult with industry formally and informally and are generally considered by the private sector to be competent, open, and co-operative. Competent authorities have also organised PPP meetings on a regular basis with the Banking Association, which, inter alia, have covered topics related to TFS. Overall, supervisors promote a clear understanding of AML/CFT obligations and risks.

FMA

Training and outreach

630. Regular training sessions, seminars and conferences have been offered by the FMA over the review period. FMA staff have also delivered training/presentations as part of private sector events organised by representative bodies.

631. Regular meetings are held with sector associations.

General and sector-specific guidance

632. The main guidance documents issued by the FMA are: (i) FMA Instruction 2018/7, which provides interpretation of, and guidance to support, the DDA/DDO and has sections specific to various sectors and sub-sectors; and (ii) FMA Guideline 2013/1, which provides guidance specifically on the implementation of a risk-based approach. Both documents are extensive and detailed and confirmed by industry as being a useful resource. A list of other relevant guidance documents is given at R.34 in the TC Annex.

633. In addition, the introduction of DDA Risk Tools – business and customer risk assessment templates - has proved to be an effective way of raising standards. Originally intended to support customer risk assessments by TCSPs, these were designed by the FMA with input from the private sector and are now tailored for each sector. Industry confirms that these templates, which include risk factors and weightings, have led to a more sophisticated approach to customer risk assessment, and in some cases to significant re-classification of existing as well as new customers. The template also serves as a starting point for business risk assessments in the TCSP sector (a business risk assessment template has been developed by the Institute of Professional Trustees in collaboration with the FMA) and is used as a benchmark in other sectors.

Chamber of Lawyers

634. Recently, the Chamber of Lawyers has started to offer a course for lawyers on AML/CFT with the University of Liechtenstein. The course is offered twice per year and is attended also by candidates for the bar exam. Each course has 20 participants on average.

Overall conclusions on IO.3

635. There have been some positive developments in the supervisory approach followed by the FMA since the last MER, in particular the introduction of a specific risk model and overhaul of its inspection model from 2019. The AT has focussed on the post-2019 approach and has given more weight to findings in relation to this latter period. These developments, together with entry controls and evolving policy on the application of administrative sanctions (monetary fines) place the FMA in a strong position to demonstrate substantial effectiveness.

636. However, the AT has significant concerns about the planned and actual frequency of inspections of higher risk entities, particularly TCSPs, which are not currently supported by sufficient resources. The AT is also not convinced that sufficient use of sanctions has been made in the TCSP sector given the risk and levels of compliance noted during the period under review. This sector is considered to be the most important sector in Liechtenstein, along with banking.

637. Whilst the supervisory model for lawyers is comparatively rudimentary, given the risk and size of the regulated sector, little importance has been attached to shortcomings highlighted.

638. **With these concerns in mind, Liechtenstein is rated as having a moderate level of effectiveness for IO.3.**

7. LEGAL PERSONS AND ARRANGEMENTS

7.1. Key Findings and Recommended Actions

Key Findings

Immediate Outcome 5

a) Setting up a legal person or legal arrangement in Liechtenstein is straightforward and detailed information is available publicly on the creation and types of legal persons and arrangements from the websites of the Office of Justice and Liechtenstein Marketing.

b) The authorities acknowledge that legal persons and legal arrangements can be misused for ML/FT purposes. They have a good broad understanding of the risk that legal persons (and legal arrangements) may be used to launder the proceeds of crime. There is less granular, documented understanding in respect of the risk of TF.

c) The authorities rely on a range of measures to prevent the misuse of legal persons and legal arrangements, e.g., the recently introduced register of BO information and obligation placed on legal persons that are predominately non-trading and wealth management structures (around 80% of legal persons) to appoint a "qualified member" to the governing body, who is responsible for compliance with BO obligations and actively involved in day-to-day management. Measures are effective in helping to prevent the misuse of legal persons and legal arrangements.

d) Basic and BO information is available from two sources: (i) registers maintained by the Office of Justice; and (ii) directly from the private sector. In practice, BO information has generally been obtained by competent authorities directly from the private sector (including qualified members of legal persons), and law enforcement also from legal persons and legal arrangements, and the BO register used as a secondary source.

e) The AT considers that basic information held by these sources is generally accurate and up to date. However, basic information in the commercial register is held only for trusts created for a period of more than twelve months.

f) A BO register and related legislation have been in place since August 2019. With few exceptions, e.g., for trusts where there may be long delays in filing information, adequate BO information on legal persons and legal arrangements is already held on the BO register. Whilst the Office of Justice is expected to proactively monitor the completeness and plausibility of information held on the register, it had not done so at the time of the on-site visit and, instead, reliance was placed on qualified members of legal persons to submit accurate information on a timely basis. While the results of supervisory activity do not indicate particular issues in compliance with BO obligations, the AT is concerned about the continued level of supervision of TCSPs, including qualified members, and considers that there has been insufficient oversight of the performance of CDD activities by qualified members. This alternative to proactive oversight by the Office of Justice is therefore not

considered to be sufficiently effective in demonstrating that BO information held in the register is accurate and up to date.

g) These shortcomings would not matter, or matter less, if combined access to information held in the BO register and BO information held by the private sector cumulatively ensured the availability of adequate, accurate and current information. However, BO information held by the private sector – which updates information based on risk – will not necessarily be up to date.

h) There have been no obstacles or difficulties accessing basic or BO information in a timely manner.

i) Sanctions taken in respect of failures to comply with basic information requirements of the Persons and Companies Act are considered to be effective, proportionate, and dissuasive. However, administrative fines applied for failing to provide BO information are not considered to be effective, proportionate, or dissuasive.

Recommended Actions

Immediate Outcome 5

a) The authorities should undertake a more in-depth analysis of the risks that legal persons and legal arrangements could be used for TF, including the inherent vulnerabilities of all the different types of legal persons and arrangements and activities.

b) In line with practice started post on-site, the authorities should continue to apply compliance checks to ensure: (i) accurate and up to date information is being provided to the BO register; and (ii) discrepancies are being reported by the private sector, periodically reviewing effectiveness. A similar approach should be considered for basic information.

c) In line with an already agreed approach, the authorities should apply a mixture of higher fines, particularly for professional directors, and dissolution or liquidation of legal entities for failure to submit BO information.

d) The authorities should reduce the period in which to register or notify a trust in or to the Commercial Register (currently twelve months from establishment).

639. 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, and elements of R.1, 10, 37 and 40.[33]

[33] The availability of accurate and up-to-date basic and BO 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.

7.2. Immediate Outcome 5 (Legal Persons and arrangements)

640. Liechtenstein's legal framework provides for the establishment of a wide variety of legal persons including (in order of use): foundations, establishments (Anstalten), and public limited companies. Numbers of legal persons and legal arrangements created in Liechtenstein at the end of 2020 are set out in a table in Chapter 1. Legislation also provides for the creation of types of legal person in addition to those listed in the table which have never been used in practice, such as companies limited by units, mutual insurance associations, auxiliary funds (linked to mutual insurance), unregistered partnerships and communities of property. With regard to legal arrangements, the Liechtenstein legal framework provides for the establishment of trusts, but no other comparable arrangements.

641. Foundations are often used in connection with holding structures that include both domestic and foreign legal persons. The formation and administration of legal persons is a core business of TCSPs. The majority of legal persons and legal arrangements are used by foreign residents.

642. While there has been a significant reduction in the number of legal persons and legal arrangements registered or otherwise domiciled in Liechtenstein during the period under review (68% decrease in number of legal persons and legal arrangements over the past 13 years), there is no suggestion that greater use is being made of foreign legal persons or legal arrangements administered from Liechtenstein. The fall is due in particular to measures taken to improve tax transparency. See Chapter 1.

7.2.1. Public availability of information on the creation and types of legal persons and arrangements

643. Information on the creation and types of legal persons and legal arrangements is publicly available.

644. The different types, forms and basic features of legal persons and legal arrangements are set out in various legislation, mainly, but not solely, the Persons and Companies Act. These are described in detail at c.24.1 in the TC Annex. All Liechtenstein laws, including any amendments thereto, are promulgated in the Liechtenstein Law Gazette (LGBl) and are accessible free of charge, including via its website. In addition, laws of more relevance to the finance sector are translated into English and available on the Liechtenstein Government's website.

645. Detailed information is also available publicly on processes for creation and types of legal persons and legal arrangements from the websites of the Office of Justice and Liechtenstein Marketing (a public law entity that is entrusted with the marketing of Liechtenstein as a business and tourism destination). Factsheets published by the Office of Justice were last updated in January 2021. These contain details of the preparatory work required for formation/registration, documents to be submitted (including a description of their content), formation procedures and fees to be paid.

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

646. The authorities acknowledge that legal persons (and legal arrangements) can be misused for ML/FT purposes, in particular that such vehicles have been used to obscure BO. They have a

good broad understanding of the risk that legal persons (and legal arrangements) may be used to launder the proceeds of crime. There is less granular, documented understanding in respect of the risk of TF.

647. Detailed analysis on how legal persons (and legal arrangements) could be used for ML purposes was conducted in 2019 and was finalised and shared with relevant stakeholders in May 2020: "Analysis of money laundering risks of Liechtenstein entities" (139 pages). This was the country's first specific analysis of ML risk posed by legal persons (and legal arrangements). The risk assessment was comprehensive and based on an assessment of threats, inherent risks and risk-mitigating measures, and tackled issues such as use of bearer shares, powers of attorney, and use of shell companies and complex structures. After taking into consideration the risk mitigating measures in place, a residual ML risk level of "medium" was determined. This rating is consistent with the AT's view. Chapter 2 (IO.1) also considers this risk assessment.

648. The risk assessment did not consider the risk that Liechtenstein trusts may be declared or settled outside the country, with no link to Liechtenstein other than use of its legislation. The shared view of competent authorities and industry practitioners (and also the AT) is that this is very unlikely to occur in practice for trusts given that much greater use is made globally of Anglo-Saxon trust law and BO notification requirements that still apply.

649. There has been no corresponding specific report in relation to how legal persons (and legal arrangements) could be used for TF purposes. Rather, the authorities produced a national TF risk assessment in May 2020 (NRA-TF). This mainly covered general TF risk – for instance extensive analysis is included in relation to fund flows - but this did not distinguish any threats specifically connected to legal persons (or legal arrangements). The TF risk level of legal persons and arrangements was determined as "medium-low". This rating is consistent with the AT's view.

650. Some analysis specifically on the risk that legal persons (and legal arrangements) could be used for TF was included as a section in NRA-TF (section 4.5.2; approx. 2 pages). This consisted of a comparatively limited analysis of TF threat, focussing on identified connections of existing legal persons and arrangements to high-risk countries. This involved reviewing information on the relevant registers and identifying whether: (i) any involved parties (e.g., directors, foundation members) were nationals of, or residing in, the capital cities of high-risk countries; and (ii) any of these countries were mentioned in the statutory documents of the legal person or legal arrangement.

651. Other than in a separate NPO risk assessment, there was no consideration of the different inherent vulnerabilities of all the different types of legal persons and legal arrangements or their activities for TF purposes, as the authorities consider that legal persons and legal arrangements (irrespective of their legal form) could all be misused in the same way. The AT do not consider the approach followed for the assessment of TF risk to be sufficient.

7.2.3. Mitigating measures to prevent the misuse of legal persons and arrangements

652. The authorities rely on a range of measures to prevent the misuse of legal persons and legal arrangements, including those to ensure that BO information is available, e.g., the recently introduced register of BO information, and obligation placed on legal persons (excluding partnerships) that are predominantly non-trading and wealth management structures (around 80% of legal persons) to appoint a "qualified member" to the governing body under Art. 180a of the Persons and Companies Act. The latter, in particular, presents a particular hurdle to those

looking to establish a legal person for the purpose of misusing it for ML/TF. In addition, and by way of context, recent changes related to tax transparency rules also appear to have acted as a general deterrent to the misuse of legal persons and legal arrangements - as evidenced by a significant decrease in numbers registered or notified to the Commercial Register Division compared to the last MER (see Chapter 1). These measures are effective in helping to prevent the misuse of legal persons and legal arrangements.

653. The BO register – established in August 2019 and operated by the Office of Justice - provides up-to date information, although some technical gaps have only recently been, or are still in the process of being remedied, i.e.: (i) the obligation to provide information on all founders/settlors; (ii) the application of obligations to partnerships; (iii) the obligation placed on FIs, DNFBPs, VASPs and competent authorities to notify discrepancies; and (iv) compliance checks by the Office of Justice. See section 7.2.4 below for more detail.

654. The extensive use of the Art. 180a regime is an effective measure to mitigate risk. This regime covers around 80% of legal persons, predominantly non-trading and wealth management structures. Requirements do not extend to legal persons that hold a licence under special legislation (see below) or partnerships (of which there are just a limited number). All legal persons covered by the regime must appoint at least one qualified member to their governing body. These qualified members (professional trustees or persons licensed under the 180a Act – referred to collectively as TCSPs) are subject to the DDA (and so required to apply preventive measures) and are licensed and supervised by the FMA for AML/CFT purposes.

655. There are approximately 215 individuals authorised to act solely as a qualified member in Liechtenstein. Around 66% of these are employed by a TCSP and make use of the systems and controls and infrastructure of the TCSP in fulfilling their Art. 180a function for multiple entities. The remaining 33% are "independent", although this number has been decreasing with no new licenses issued for independents since 2014. Independent qualified members typically service 4 or 5 entities with which they have a long-standing relationship (e.g., family foundations).

656. These qualified members are required to find out and verify the identity of the BO of the legal person to which they are appointed. Whilst the qualified member is not legally responsible for providing BO information to the Office of Justice, they regularly fulfil this role in practice (see 7.2.4). In addition, as a member of the governing body, they are also actively involved in the day-to-day management of the legal person and act as a professional director, with full voting rights, executive authority, and fiduciary responsibilities.

657. As a result, services provided by TCSPs are generally "full scope/full service" and there is very little appetite for the provision of more limited services (e.g., provision only of business and postal addresses or acting as representative to a trust) where it may be harder to monitor ongoing activities. Given their higher cost base in Liechtenstein, it is not economic for TCSPs to provide such a limited service.

658. Although it is possible for a qualified member to delegate effective authority (for instance, delegating signing authority or powers of attorney to a settlor/founder) this is largely a decreasing historic position and does not commonly occur in practice.

659. In relation to those legal persons where an Art. 180a qualified member is not required to be appointed (around 20% of cases), all hold a licence in Liechtenstein pursuant to legislation, e.g., under the Business Act (generally manufacturing or commercial entities). They must have a physical operation in Liechtenstein. ML/TF risk in these entities is comparatively low and is

largely managed by the business licencing process, e.g., by the Office of Economic Affairs, which includes checks on BO and management, site visits (through a team of inspectors) and liaison with other agencies where necessary – in order to monitor compliance with business legislation.

660. The Commercial Register Division is responsible for checking that legal persons meet the requirement to appoint a qualified member. It does so at the time that a new legal person is registered and every time that there are changes to the composition of the governing body. It also works closely with the FMA and is made aware - on an ongoing basis - of new licences, lapses, and termination of licences under the Trustee Act or 180a Act. In addition, every six months the Commercial Register Division reviews compliance with the regime by all legal persons. It acts where there is failure to appoint a qualified member - see Section 7.2.5 – allowing a legal person two months in which to regularise its position (and an additional two months in cases where proven efforts are being taken). Whilst this timeframe is understandable, it is possible that benefits of the Art. 180a regime may be undermined. The Commercial Register Division does not enforce the requirement with respect to associations (of which there are a limited number).

661. Whilst the Art. 180a regime does not apply to trusts, around 94% of trusts (April 2021) with a trustee resident in Liechtenstein have appointed a professional trustee that is subject to the DDA – in line with the Trustee Act. Whilst the authorities have not conducted an in-depth analysis of the operation and/or activities of the 6% of trusts that do not have a professional trustee, they are aware that these are "family trusts", in which family members act on a non-professional basis. No other examples are known to the authorities and no other types were identified in discussions with TCSPs.

Shell Companies

662. As noted elsewhere in this MER, Art. 165 of the CC was amended in 2019 (see section 3.3.2) to include tax savings as asset components subject to ML (the absence of which had been identified as a vulnerability). The effect of this has been to dramatically curtail the private sector's appetite for using shell companies (which may be used in schemes to perpetrate tax offences), with industry participants describing numerous banking relationships being terminated where true substance could not be established. The Office of Justice is not able to identify which companies in the Commercial Register are shell companies and so it is not possible to quantity the reduction in use.

Bearer sharers

663. While bearer shares may be issued by public limited companies, partnerships limited by shares and European Companies, they must be deposited with an appointed custodian, which is subject to an annual audit. This requirement and limited exemptions thereto are set out under c.24.11. Based on an analysis by the authorities, there are currently no companies domiciled in Liechtenstein that have issued bearer shares that could use these exemptions and so this has not materially affected effectiveness.

7.2.4. Timely access to adequate, accurate and current basic and beneficial ownership information on legal persons and arrangements

664. Basic and BO information on legal persons and legal arrangements is obtained from two sources: (i) registers maintained by the Office of Justice; and (ii) directly from the private sector.

665. In practice, whilst BO information has been obtained by competent authorities through the BO register, those authorities also seek BO information directly from the private sector

(generally TCSPs and banks) and law enforcement also from legal persons and legal arrangements, and the BO register is often used as a secondary source to verify BO information obtained directly from the private sector. The reason for obtaining BO information directly from the private sector is that it is possible to access also non basic/BO-specific information at the same time, such as a complete CDD file, business profiles and transactional data, rather than because of any particular concerns about information held in the BO register.

666. Except for trusts created for a period of twelve months or less, adequate basic information (excluding information on shareholders) on legal persons and legal arrangements is held on the register at the Commercial Register Division and is available publicly. Information on registered shareholders is available directly from legal persons and on bearer shareholders from custodians. Overall, based on information presented below, the AT considers that information held by these sources is generally accurate and up to date.

667. Adequate BO information has been held on the BO register at the Office of Justice for the vast majority of legal persons and legal arrangements. However, as explained below, the authorities have not demonstrated that sufficient measures have been in place during the period under review to ensure that this information is accurate and current. Whilst BO information has also been available directly from the private sector, as explained below, this information may not always be accurate and up to date.

668. These shortcomings would not matter, or matter less, if combined access to information held in the BO register and BO information held by the private sector cumulatively ensured the availability of adequate, accurate and current information (i.e., the whole is greater than the sum of the parts). However, this has not been demonstrated by the authorities.

669. There have been no obstacles or difficulties accessing basic or BO information in a timely manner.

Basic information – Commercial Register

670. All legal persons and legal arrangements, except a very small number of legal persons (see c.24.1 and c.24.3) and trusts created for a period of twelve months or less must be registered or, in the case of non-registered foundations and non-registered trusts, required to notify the Commercial Register Division of formation, including basic information. Both registration and notification involve the provision of basic information as prescribed under c.24.3, but in the case of trusts created for a period of more than one year, it may take up to one year to file the necessary information, though in practice shorter filing periods have been observed.

671. Basic information on Liechtenstein legal persons and arrangements held by the Commercial Register Division is publicly available and accessible online.

672. Legal persons and legal arrangements are required to notify the Registrar of changes to basic information "without delay" (interpreted to mean as soon as possible – see c.24.5), while non-registered foundations must notify any changes to information previously notified within 30 days – certified in writing by an attorney, professional trustee or a person licensed to do so under the Art. 180a regime. The Commercial Register Division reviews all documents presented and satisfies itself that requirements to provide basic information are met.

673. Whilst the Commercial Register Division has powers to examine entries in the commercial register, it does not proactively check the accuracy/plausibility of information that it collects or that changes to data held are notified to it without delay (or as otherwise provided). Instead, the

following mechanisms are used in practice to support accuracy of basic information maintained in the commercial register : (i) the "constitutive" effect of registration of information (except for non-registered foundations and trusts) - which means that a change to basic information does not have legal effect until registration, which ultimately encourages (timely) submission of changes (see c.24.5 in the TC Annex); (ii) checks by other public authorities, e.g. the FMA - which identify cases where information held is inaccurate; (iii) STIFA onsite inspections – which verify the accuracy of basic information that is held in the commercial register in respect of non-registered private benefit foundations, which account for approximately 40% of legal entities created in Liechtenstein; and (iv) the additional assurance that is provided by the appointment of a qualified member under Art. 180a of the Persons and Companies Act - whereby a professional director sits on the board of a large majority of legal persons, which should have a positive effect on compliance with statutory obligations. The effect of (i) is that the register is always technically up to date and accurate from a legal perspective (meaning it is enforceable) although it is possible that false information may be given to the registrar or that there is a delay in reporting changes. On average, STIFA verifies the accuracy of basic information held in the commercial register for 125 non-registered foundations per year which limits the effectiveness of this control.

674. In the case of registers of shareholders held by legal persons, all competent authorities have powers to examine entries in share registers (along with other competent authorities). In order to support the accuracy/plausibility of information held therein, the following mechanisms are used in practice: (i) the "constitutive" effect of registration of information, which means that a change to a shareholding does not have legal effect until registration, which ultimately encourages (timely) submission of changes (see c.24.5 in the TC Annex); (ii) in the case of bearer shares, an annual audit/review which verifies whether the person receiving dividends is entered in the register of bearer shares and if all information on the shareholder (name, date of birth, domicile, etc.) is entered (see c.24.11); (iii) checks by other public authorities, e.g. the FMA – which identify cases where information held is inaccurate; and (iv) the additional assurance that is provided by the appointment of a qualified member under Art. 180a of the Persons and Companies Act which means that there is at least one professional director in place to ensure that the register is accurate and that dividends are not paid to unregistered third parties (see also c.24.5).

675. Before February 2021, competent authorities had indirect access to basic information on legal persons and legal arrangements through the Commercial Register Division. This was typically provided by e-mail on the same working day as the request. Since February 2021, the FIU, FMA, Court of Justice, OPP, National Police, and the Fiscal Authority have had immediate and direct electronic access to all basic information (including supporting documents) maintained by the Commercial Register Division. Until the implementation of direct electronic access to basic information on 1 February 2021 (which is not recorded), the FIU submitted about 30 requests a week for basic information, and FMA around 40.

Beneficial ownership – Office of Justice

676. A central BO register was introduced in Liechtenstein in 2019, as part of the implementation of the 4th EU AMLD, whereby BO information is held in an electronic register

maintained by the Office of Justice for the vast majority of legal persons or legal arrangements[34]. Such legal persons and legal arrangements are obliged to establish and verify the identity of BOs on an ongoing basis, which includes keeping such information up to date, though in the case of trusts created for a period of more than one year, it may take up to one year and 30 days to file the necessary BO information following establishment (see c.25.1). In order to support this legal obligation, a requirement is placed on BOs to provide the legal person or legal arrangement with necessary information, but this requirement is not directly enforceable against the BO (see c.24.6). The definition of BO is in line with the DDA, and so it is considered by the AT that information held in the register will be adequate.

677. More recently, this registration requirement has been extended to include: (i) an obligation to provide information on all founders and settlors, as opposed to just those with controlling functions (applied from April 2021, with a 6-month transitional period); (ii) all partnerships (applied from April 2021, with a 6-month transitional period) – the majority of which are involved in manufacturing; and (iii) a requirement for FIs, DNFBPs, VASPs and competent authorities to refer to the BO register and notify discrepancies between BO information that they hold (e.g., through the application of CDD measures) and BO information recorded in the BO register (applied from 1 October 2021 to FIs, DNFBPs and VASPs). At the time of the onsite visit, the Office of Justice had not analysed what additional information was still to be provided under these transitional provisions.

678. Upon receipt of each submission, the Office of Justice verifies that the information provided is complete. It also has a power to undertake random compliance checks, to ensure that plausible information has been provided on a timely basis but had not performed any such checks at the time of the onsite visit. These checks commenced after the end of the transitional period (1 October 2021) and a concept for doing so was presented during the on-site visit.

679. In the absence of random compliance checks and requirement for discrepancies to be reported by FIs, DNFBPs or VASPs in the period under review, the Office of Justice has largely relied on qualified members of legal persons (see section 7.2.3 above) to ensure that BO information submitted by the legal person is accurate and submitted on a timely basis - in their capacity as a member of the governing body. However, while the Art. 180a regime is overall a robust and effective one and the results of supervisory activity do not indicate particular issues in compliance with BO obligations, there are concerns over the continued limited level of supervision of TCSPs, despite the sector's medium/high ML risk rating in NRA II, along with low levels of suspicion reporting and little formal sanctioning of the sector during the review period. (See IO.3 for further detail). It is noted also that there is no memorandum of understanding in place between the Office of Justice and the FMA, covering the circumstances in which information is exchanged between the two authorities in respect of the conduct of qualified members, though, as required under the DDA, the two cooperate in practice (e.g., the Office of Justice now shares concerns about particular TCSPs that may be considered by the FMA in its risk ratings).

680. Since 2019, the FMA, FIU and the OPP have had immediate and direct access to all registered information contained in the central BO register. Since April 2021, such access has been extended to include the Fiscal Authority, the Court of Justice, the Chamber of Lawyers, and

[34] The register excludes: (i) group B and C persons listed under c.24.1 which are not used in practice; and (ii) trusts administered by TCSPs in Liechtenstein that are already entered in a BO register of another EEA Member State. Transitional provisions have also applied during the period under review – see c.24.6.

the National Police. BO information was accessed 515 times by these authorities between 1 April 2021 and 20 September 2021.

Private sector - primary method for accessing information

681. In addition to information held in the BO register, BO information is available in the country (in order of use) from: (i) qualified members (TCSPs) for around 80% of legal persons; (ii) TCSPs for nearly all trusts; (iii) banks, though the authorities estimate that up to half of legal persons and legal arrangements do not operate an account with a bank in Liechtenstein; (iv) other FIs and DNFBPs; and (v) directly from other legal persons, e.g. manufacturing or commercial entities which usually have simple ownership structures. As explained above, these sources often act as the primary source of information for the FIU and law enforcement.

682. In this respect, it should be noted again that, whilst the results of supervisory activity do not indicate particular issues in compliance with BO obligations there are concerns over the continued limited level of supervision of the TCSP sector (see IO.3 for detail). Moreover, the frequency with which CDD information held in the private sector is updated is based on risk, meaning information held and accessible via this method may not always be up to date - a concern that may reduce in importance post October 2021 following the introduction of additional compliance checks on the BO register.

683. Information from the private sector is typically provided to the FIU within one week of request, and, where necessary, the same information is subsequently collected through the Court of Justice to be used as evidence (up to two weeks).

684. During the period from 2016 to 2020, the FIU and LEAs have made the following numbers of requests to the private sector in order to obtain predominantly BO information.

Table 7.1: Requests to private sector for information

Year	FIU requests	LEA requests
2016	72	54
2017	78	48
2018	295	40
2019	355	53
2020	406	55
Total	1 206	250

685. In practice, relevant competent authorities reported no obstacles or difficulties in accessing information through the private sector: all requests for information were responded to.

Box 15

CASE STUDY – Access to BO information

Type of ML case	Stand-alone ML (foreign predicate offence), laundering of CHF 178 200.
Predicate offence	Fraud (fraudulent misuse of data processing; Switzerland).
Legal persons involved	2 corporations/Liechtenstein and Switzerland; 1 Ltd./Switzerland.
How the case was identified	Analysis report of the FIU based on a SAR/STR.
BO information obtained	In an analysis report the FIU submitted BO information concerning the above-mentioned legal entities. This intelligence information was verified by seizing banking documents of a Liechtenstein bank. The submitted and seized banking documents from the Liechtenstein bank and other evidence provided by the Swiss authorities, in particular BO information, were analysed by the National Police. Information held at the bank was found to be accurate and up to date.

7.2.5. Effectiveness, proportionality and dissuasiveness of sanctions

686. The authorities are empowered to issue administrative fines and apply other administrative measures for failure to submit basic and BO information within the prescribed filing periods and submission of inaccurate information. Whilst sanctions taken in respect of failure to comply with basic information requirements of the Persons and Companies Act are considered to be effective, proportionate, and dissuasive, administrative fines applied for failing to provide BO information do not appear to be so.

687. The authorities have provided details of various administrative actions taken in 2019 and 2020 to ensure compliance with requirements of the Persons and Companies Act. These have covered failure to: (i) provide an accurate delivery address/address for legal representative; (ii) appoint a qualified member; (iii) appoint an auditor; (iv) appoint and register the custodian of bearer shares; and (v) appoint a trustee or legal representative in the case of a foreign trust. Whilst these measures do not cover all elements of basic information set out in c.24.3 and c.24.4 (since deficiencies have not been highlighted), actions are considered to support compliance with basic information requirements. Non-compliance is largely dealt with by way of orders to remedy deficiencies ("restoration of lawful state of affairs") which threaten ultimate use of dissolution or liquidation powers for both "live" and "dormant" entities. In 2019, a total of 1 057 orders were made, resulting in, inter alia, 798 cases where the lawful state of affairs was restored and 86 cases of dissolution or liquidation. Similarly, in 2020 a total of 774 orders were made, resulting in, inter alia, 473 cases where the lawful state of affairs was restored and 40 cases of dissolution or liquidation. Two administrative fines have also been imposed by the Office of Justice for non-compliance relating to one case (CHF 1 300 in total). Dissolution and liquidation are considered by the Office of Justice to be the severest measures that can be applied for failure to comply with information requirements and reference to these measures has, in practice, encouraged compliance with remedial orders.

688. Between 2016 and 2020, the Office of Justice filed also three complaints with the Court of Justice for failure by a custodian to transfer bearer shares to a successor custodian. Administrative fines were imposed in all three cases (maximum fine was CHF 2 000).

689. As noted above, STIFA inspects whether non-registered private-benefit foundations deposit notifications of formation and amendments accurately with the Office of Justice. In 2018, four administrative fines of CHF 200 each were imposed for failing to notify the death of a co-

member. STIFA also filed criminal complaints with the Office of Public Prosecutor in three cases for failure to register common-benefit foundations with the Office of Justice. These proceedings are still pending.

690. The combined effect of the use of remedial orders and threat of use of dissolution or liquidation powers is that effective, proportionate, and dissuasive sanctions have been applied.

691. In relation to BO information, the Office of Justice may impose an administrative fine of up to CHF 200 000 for non-compliance with the obligation to enter BO information in the central BO register. During the review period, 155 administrative fines were issued by the Office of Justice (including 16 to TCSPs), with 150 concerning legal persons and 5 concerning legal arrangements. The fines were imposed after the legal entities concerned failed to comply with an initial reminder and, in all cases, BO information was registered immediately after the fine.

692. The average administrative fine imposed on trading entities by the Office of Justice for failure to register BO information during the assessment period was CHF 150 and the average for companies administered by TCSPs was CHF 500. The higher amount applied to TCSPs reflects higher expectations – since they are subject to CDD requirements under the DDA. The authorities have explained that the level of fines applied reflected the relatively recent introduction of entirely new BO requirements and that higher tariffs will be applied in future.

693. Considering the importance that is now attached in Liechtenstein to transparency, the level of administrative fines applied in respect of failure to register BO information do not appear dissuasive and proportionate, particularly for those administered by TCSPs (which have professional directors). Whilst the use of dissolution or liquidation powers for failure to comply with BO information requirements appears to be dissuasive, they were not used or threatened during the review period in relation to BO requirements.

Overall conclusions on IO.5

694. The authorities have invested significant resources in developing registers for holding basic and BO information. Legislation related to the latter provides for the Office of Justice to proactively oversee compliance with filing requirements in order to ensure that information held is accurate and up to date, something that has started since the end of the on-site visit. However, during the period under review, reliance instead had been placed on qualified members of legal persons (around 80% of legal persons) to submit accurate information on a timely basis, and concerns have been highlighted about the extent to which they have been subject to supervision for compliance with CDD obligations (highlighted under IO.3).

695. In practice, the BO register has been used as a secondary source for BO information, and the FIU and LEAs have collected information directly from the private sector for reasons given above. However, here too, there are issues in relation to supervision of the TCSP sector and the extent to which BO information will be accurate and up to date (for customers that are not assessed as presenting a higher risk).

696. Shortcomings linked to IO.3 have been heavily weighted since they have a significant impact on the effectiveness of IO.5 considering the reliance that is placed on the TCSP sector, including Art. 180a qualified members, for the availability of, and access to, BO information.

697. Concerns about the application of sanctions have also been weighted more heavily given the low fines applied to TCSPs that had not met requirements to file BO information.

698. **Liechtenstein is rated as having a moderate level of effectiveness for IO.5.**

8. INTERNATIONAL COOPERATION

8.1. Key Findings and Recommended Actions

Key Findings

Immediate Outcome 2

a) International cooperation constitutes an important part of Liechtenstein AML/CFT system in view of the predominantly foreign nature of the predicate crimes to ML. The country has a comprehensive legal and institutional framework to perform international cooperation. Competent authorities demonstrated effective cooperation in providing and seeking information, both through the use of formal and informal channels, with a range of foreign jurisdictions.

b) The authorities provide and seek mutual legal assistance (MLA)/ extradition requests both in relation to ML and predicate offences in line with the threats identified in the NRA. This also extends to execution of a broad set of information requests aimed at identifying, seizing, and confiscating funds/assets. Despite the absence of a formal case management system, the requests are prioritised, processed and addressed within a reasonable timeframe

c) Some issues in relation to dual criminality requirements regarding tax evasion (see also IOs 1 and 7), could have an impact on the effective cooperation. Several measures aimed at diminishing these risks (i.e., proceeds of tax evasion committed abroad being laundered through Liechtenstein FIs, DNFBPs or VASPs) have been implemented in recent years. Whilst their overall effect of these measures is very positive, some concerns remain if they are fully commensurate with the risks the country faces as an IFC.

d) The legislation guarantees the right to the entitled party(ies) in MLA proceedings to be heard before the court (and thus suspects and their associates could be indirectly informed of an on-going investigatory action) prior to the execution of an incoming MLA request. Since July 2021 the amendments to the MLA Act were introduced and they aim at minimising the tipping off risks deriving from these provisions. The amendments provide the possibility to the Court of Justice to issue a prohibition order to persons subject to the DDA with regard to disclosing any information concerning the documents/materials they had to share with the competent authorities as well as a possibility to transmit the relevant objects, documents and data to the requesting authority before hearing the entitled parties. The right to be heard can be postponed for a maximum of 24 months.

e) LEAs participate in formal and informal cooperation directly or via Interpol and other cooperation platforms, including through the trilateral cooperation treaty with Austria and Germany. Joint investigative teams may be formed if needed. There is also smooth cooperation between supervisors and foreign counterparts regarding market entry and consolidated supervision.

f) All incoming requests are regularly shared with the FIU and these requests represent an important basis for FIU analysis and ML investigations, when the case is conducive to further

investigation. The FIU spontaneously disseminates and pro-actively seeks information exchange with its foreign counterparts (especially from 2018 onwards) for the purposes of its own analysis of suspicious money flows.

g) Competent authorities actively exchange basic and BO information on legal persons with their counterparts. The AT did not identify any obstacles in providing this type of information.

Recommended Actions

Immediate Outcome 2

In order to further expedite all forms of international cooperation Liechtenstein should:

a) Introduce written procedures/guidance on the exact *modus operandi* to be followed by the competent authorities when receiving MLAs related to fiscal matters (regardless of if in a concrete case dual criminality principle applies). Responses to the requesting state should provide scope of information/administrative assistance that can be obtained from the Fiscal Authority. The authorities should also consider developing a standard template form for responding to these MLA requests.

b) Develop written guidance for the implementation of prohibition orders in line with the 2021 amendments to the MLA Act with a view to minimising the risk of tipping off.

c) Develop formal prioritisation criteria for all incoming MLA requests and where necessary introducing case management systems.

d) Provide publicly available guidance on the process to be followed when seeking MLA and extradition to assist non-EU foreign counterparts.

699. 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 and elements of R.9, 15, 24, 25 and 32.

8.2. Immediate Outcome 2 (International Cooperation)

8.2.1. Providing constructive and timely MLA and extradition

700. Liechtenstein has in general provided constructive and timely mutual legal assistance (MLA) and extradition across the range of international co-operation requests. Based on the feedback from the global network membership, Liechtenstein authorities provide good quality cooperation to a large extent.

701. Given the predominantly foreign nature of predicate offences to the ML (most prevalently fraud, criminal breach of trust and embezzlement, tax offences, corruption, and drug related offences) international cooperation plays a particularly important role for Liechtenstein in the framework of the overall AML/CFT efforts. In particular, as identified under the NRA threats analyses around 69% of the ML cases initiated during the period under review involved the laundering of predicates committed abroad, including around 97% of total assets blocked. Cooperation is provided and sought based on a wide range of international and domestic legal instruments (see R.36 to 39) and in application of the principle of reciprocity. While no guidance has been developed for foreign countries on the process of making MLA requests to the country,

Liechtenstein has made available useful information to assist counterparts in the respective process through the platforms of Eurojust, European Judicial Network, StAR/World Bank. In addition, there are regular contacts between foreign public prosecutors and the local OPP regarding formalities for requests for MLA. The Office of Justice, in its turn, provides support on demand in transmitting checklists for foreign authorities to guide them in drafting MLA requests.

MLA procedures

702. The Office of Justice acts as the central authority for receiving MLA and extradition requests. With the Schengen Agreement coming into force in Liechtenstein it is available to send MLA requests of foreign law enforcement authorities directly to Liechtenstein Court of Justice as well. This channel is also available for cooperation with Austria, Germany and Switzerland based on bilateral agreements with these countries. Those requests which are not governed by the Schengen agreement and bi/multilateral agreements (e.g., MLAT with the United States) usually go through diplomatic channels or directly to the Court of Justice. The Office of Justice, based on established processes, runs a database, where it registers the requests on the day of receipt and forwards it to the Court of Justice for execution. The Office of Justice examines the formal requirements of the request and decides on its execution as provided under the MLA Act. No appeal can be lodged against decisions of the Office of Justice.

703. As regards the Court of Justice, no separate procedures have been developed for the latter to deal with MLA requests, its actions are governed by the Judicial Act and MLA Act. There are 4 judges assigned for execution of MLA requests. When a request is received it is registered with the Court database and a file is opened together with the form of respective assignments of the judge. On receipt, a copy of the request MLA is submitted to the OPP which, within the scope of its own competence in matters of MLA, also monitors that the request is attended to promptly. The FIU (for ML/TF and predicate offences) and the Fiscal Authority (for fiscal offences) also receive copies of incoming requests. Overall, the system appears to be effective. Despite the absence of a formal case management system, the requests are processed and addressed within a reasonable timeframe. The resources made available for responding to MLA requests seem to be sufficient and there are no practical or legal obstacles. An opened file is assisted to one of the judges by a secretariat member per judge. On average, 289 MLA requests are sent to the Court per year, which are divided between 4 judges. It takes around 73 days to execute a request.

Prioritisation

704. There is no specific legislative provision or instruction concerning prioritization of individual cases. As explained by authorities this is due to the issue of not affecting judicial independence. In practice, requests for MLA are presented to the competent judge on the day of receipt, who, as a general rule, inspects the request for MLA and decides on its urgency that same day, in particular if the request for MLA has been marked as urgent or in the case of requests where the urgency is evident. All requests are assessed to determine their level of priority and urgency based, *inter alia*, on the nature of the requests, the seriousness of the offence and the urgency of the case. At that, requests for arrest and extradition, freezing, the ones requiring actions by foreign partners and those requests where there is risk of loss of evidence are dealt with as a priority (in 2 days in case of asset freezing).

705. Admissibility of the requests as per its formal requirements is assessed based on Art. 14 of the ECMA, as well as the MLA Act in case of absence of an MLAT. In the event of a likely refusal, the applicant jurisdiction is assisted in perfecting its request. In that event the improved request

can be provided to the Court with supplementary information and on repeated occasions, if necessary.

Refusals

706. With regard to the grounds for refusal, the MLA requests can be refused on the basis of provision of insufficient facts on the case to examine mutual judicial criminal liability, if the execution would violate the public order, the request is based on military or political offence, the offence is not punishable under Liechtenstein law. As advised by the authorities many refusals are related to the insufficient formal requirements, where the requesting authorities are informed about the shortcomings in writing, in case of German speaking countries via phone call, and are requested to make the necessary improvements. In case of incomplete remedy of the shortcomings, the MLA is provided partially, to the extent possible. Any refusal has only a relative effect and does not prevent the requesting state from repeating its request at a later time. Authorities advise that assistance is very rarely refused on the grounds of a political or military offence and the violation of public order.

707. Dual criminality, as per authorities, is also a rare ground for refusal. Regarding tax offences, since 2016 Liechtenstein provides MLA if the dual criminality is met and if the circumstances of the case described in the MLA request would be punishable in Liechtenstein. The authorities advised that very often the MLA request on fiscal offences is captured by the Liechtenstein legislation and thus the MLA is provided. In case an MLA request related to tax offences is received the Fiscal Authority is also involved in the process for proper qualification of the case. The authorities also provided a case example of execution of an MLA related to tax offences with the involvement of the Fiscal Authority.

Case study- Response to a tax related MLA request with the involvement of Fiscal Authority

In July 2020, Liechtenstein received a request for MLA from neighbouring country in relation to suspected tax fraud and tax evasion, partly attempted, partly completed. The request was brought to the attention of the Fiscal authority for its comment. Three days later, the statement of the Fiscal authority was received by the Court of Justice, confirming that tax fraud (Art 140 of the Tax Act) was to be assumed under Liechtenstein law, because there were fictitious legal transactions as a result of a de facto self-dealing. As a result, coercive measures were ordered by the Court of Justice, including a house search, freezing of funds on bank accounts and seizing of banking documents.

708. The AT commends the initiatives undertaken by the country to mitigate the risks arising from tax offences however the concerns expressed under IO.7 are also valid in the context of provision of cooperation. At that, the AT is not fully convinced that the measures taken are commensurate with the risks the country faces as an IFC with the potential of domestically laundering proceeds of foreign tax evasion. This is further confirmed by the findings of the NRA, which identifies foreign tax offences as posing medium-high level of risk, with *"… a risk of income and assets of foreign customers not being declared or not fully declared…"*. In this regard while the case provided by the authorities demonstrates that the country has provided cooperation, it also shows that cooperation was provided only on the part of tax fraud, but not in relation to tax evasion (MLA was requested based on tax fraud and tax evasion).

709. As regards the practical number of refusals, out of 93 refusals for the period of 2015-2019, the majority were on the ground of lack of sufficient facts and circumstances to justify the

suspicion, while 29 refusals were related to lack of dual criminality for non-qualified or simple tax evasion. Whilst the dual criminality presented a basis for refusal of MLA, these cases were not dropped automatically but the authorities tried their best to focus on what could be done at the level of administrative assistance. In this regard case examples were presented to the AT demonstrating that such assistance was provided whenever MLA request would target fiscal matters not criminalised in Liechtenstein (i.e., tax evasion). Authorities further advised that as a matter of practice each refusal letter from the Court of Justice that communicates a denial of MLA due to the lack of dual criminality, informs simultaneously about the alternative way of requesting administrative assistance in tax matters from the Fiscal Authority. In addition, authorities advised that this is a standard practice followed by all competent judges in line with the requirements of Art. 56a of the MLA Act which stipulates that an MLA request referring to a fiscal offence must be transmitted by the Court of Justice to the Fiscal Authority for comment. This being noted, the AT is of the opinion that written procedures should be introduced on the exact modus operandi to be followed by the competent authorities in all cases where MLA requests in relation to tax offences are refused due to the dual criminality issues. This would ensure effective cooperation to a widest extent possible.

Confidentiality

710. As per the confidentiality of MLA requests (and thus the related investigations), the current legislation provides that 'entitled party(ies)' must be granted a hearing before the Court of Justice decides to render MLA, i.e., to render evidence gathered as per the request (Art. 55 para 4 MLA Act). The issue of possible tipping off in these cases has been discussed with the competent authorities and, for this purpose, the AT took note of the relevant provisions of the amended MLA Act and its explanatory note (see also R.37 – C.37.6). For reasons of investigative tactics, it is important that the persons concerned (referred as 'entitled parties' in the MLA Act) either do not gain knowledge of the proceedings or that their involvement (e.g., through their provision of documents/information to the competent authorities) does not bring a tipping off risk. 'Entitled parties' include all parties affected by an MLA request – usually these are persons subject to the DDA from whom specific information/documents are requested, but 'entitled party' can also include suspect(s) – he/she/they become entitled party(ies) if, for example, information on his/her/their bank account(s) is requested via MLA. Relevant legislation provides that 'entitled parties' must be granted a right to be heard before the judicial authorities, prior to handing over the information to the requesting state. This brings a tipping off risk and may lead to destruction of evidence by suspects and their associates. At the same time, it should be noted that even when the investigation is not confidential, the possibility of appeal by the entitled parties may slow down the MLA procedure. The authorities confirmed, that while this has not happened very often (mostly due to absence of domestic address of the concerned parties), in cases where this right has been exercised by defendants, it prolonged the execution of requests for at least few months. The AT discussed and analysed this issue and cases it concerned, in light of both – effective ML investigations/prosecutions and provision of international cooperation. Competent authorities are aware of these risks, and they invest efforts and resources to establish appropriate investigative tactics to avoid them. Further to this, the MLA Act was amended in July 2021 and now provides that the Court of Justice may issue a prohibition order (prohibition of disclosure) to the person subject to the DDA from whom documents/information were requested. This prohibition means that they must not inform anyone (including suspects) of the procedure and information/documents requested from them by the competent authorities. This prohibition may last for a period of 24 months. More importantly, the Act now provides for the possibility to

transmit the relevant objects, documents, and data to the requesting authority whilst the 'entitled party' would be heard before the court only after the prohibition of disclosure has been lifted. This development is expected to minimise the tipping off risks and the authorities are encouraged to continue with their efforts in this direction.

Provision of MLA

Table 8.1: Incoming MLA requests by countries

Requesting state	2016	2017	2018	2019	2020
Switzerland	90	72	83	72	75
Austria	105	77	40	42	56
Germany	48	43	27	32	47
Poland	6	11	14	8	13
Netherlands	8	13		7	
Slovenia	10	12	10	6	6
Czech Republic	8		7	7	7
Ukraine	-	8	6	5	8
Italy	6	10	-	-	8
Spain	8	6	-	5	-
United States	-	-	8	11	-
United Kingdom	-	6	-	-	5
Russian Federation	-	-	8	-	-
Latvia	-	-	-	-	8
Hungary	-	-	7	-	-
Total	**307**	**258**	**210**	**195**	**233**

711. Statistics illustrate Liechtenstein's active international co-operation. From 2016 up until 2020, Liechtenstein received a total of 1447 MLA requests, whereby 1153 MLA requests (excluding extradition) came from neighbouring countries- Austria, Germany, and Switzerland, with relatively lower number also coming from Slovenia, Poland, Netherlands. Requests concerning ML, fraud, corruption, drug trafficking, and theft and robbery were top crimes incoming MLA requests concerned most commonly. As provided in the table below, Liechtenstein demonstrated a good rate of execution of the MLA requests. As illustrated in the statistics, the number of requests related to the main proceeds generating crimes throughout the years stayed relatively the same.

Table 8.2: Incoming MLA – Offences the subject of MLA requests

	2016		2017		2018		2019		2020	
Offence	rec.	exec.	rec.	exec.	rec.	exec.	rec.	exec.	rec.	exec.
ML	65	57	90	72	80	71	75	70	85	76
Fraud	188	179	192	187	169	168	169	164	168	158
Tax offences	21	17	26	18	8	6	13	6	21	12
Corruption and bribery	19	18	27	22	19	15	21	20	17	16
Drug trafficking	10	9	8	8	10	10	19	18	16	15

Criminal group/ organisation	25	22	22	21	19	17	19	17	19	16
Robbery or theft	15	15	10	10	19	19	21	20	13	12
Total	343	317	375	338	324	306	337	315	336	305
Execution ~		***92%***		***90%***		***94%***		***93%***		***91%***

712. The statistics demonstrate that the numbers of incoming requests on foreign predicate offences is consistent with the findings of the NRA II as per the level of threats posed by these predicates for ML.

713. As demonstrated by case examples the country has the capabilities to deal with a variety of MLA requests for various forms of assistance, including taking evidence from persons, executing searches and seizures, providing information and evidentiary items, providing originals or certified copies of relevant documents and records, including administrative, bank, financial, corporate, or business records, identifying or tracing proceeds of crime, etc. International cooperation has also very often been used as a source of information leading to domestic investigations and prosecutions, with these criminal proceedings regularly resulting in confiscation (please also see IOs 6, 7 and 8 for respective case examples).

Case Study 1- Incoming MLA resulting in a domestic investigation and forfeiture
In the context of an MLA request from country A, a forfeiture order was executed in respect of assets in a Liechtenstein bank account. The account in question was attributable to the mother-in-law of a perpetrator who had been convicted of multiple offences related to organised crime in the country A. Based on an SAR/STR an investigation was launched in Liechtenstein against the wife for ML concerning the assets on the bank account mentioned above. An MLA request was sent to the country A, which enabled them to initiate new proceedings resulting in judgements, which have been requested to be enforced in Liechtenstein. A renewed forfeiture was ordered against the husband, on the assets held in the Liechtenstein bank account, as they originated of his crimes. This decision could then be enforced in Liechtenstein by means of a request for MLA dated March 2017, whereby approximately USD 1.1 million were declared forfeited in July 2017. The decision was not appealed and became final.

Case Study 2- Incoming MLA resulting in forfeiture with the involvement of several countries and complex structures
Proceedings in four countries against different persons, including in Liechtenstein were initiated on the award of contracts for the supply of war material, suspicions of corruption against involved natural and legal persons arose. The investigation was opened in June 2008 against the BOs of two foundations. They were presumably involved in the execution of the offences and transferred assets and received compensation. This remuneration ultimately went to Liechtenstein, to the benefit of two foundations, which maintained bank accounts there. Attempts were made to obtain more information through multiple requests for MLA sent and received to the countries involved. The nationals of country A were convicted in country A for aiding and abetting bribery, fraud and other offences and a forfeiture order was then issued against the mentioned foundations in Country A in 2017. In December 2017, the Country A authorities subsequently applied for the enforcement of that decision, which was carried out by decision of January 2018. The decision was not appealed and became final. A total of approximately EUR 980 000 was recovered.

MLA on asset recovery

714. The legal framework and procedures on enforcement of foreign pecuniary orders, as well as detailed statistics on practical application of freezing/ forfeiture powers by Liechtenstein authorities based on an MLA request, are provided under IO.8. Once there is a forfeiture (or confiscation) decision in criminal proceedings from the court, objects (instrumentalities) and assets which have been seized and frozen devolve upon the State of Liechtenstein. The same is true for the enforcement of foreign pecuniary orders, which also devolve upon the State of Liechtenstein (Art. 64 para 7 MLA Act). Art. 253a CPC provides that in the case of offences committed abroad, the Government can conclude an agreement with the State where the offence was committed with respect to the sharing of forfeited or deprived assets and can, in particular, include conditions in such agreement concerning the use of such assets. Pursuant to Art. 253a para 2 CPC the Government is responsible for the execution of these sharing agreements. In the case of the embezzlement of public funds, the international obligation resulting from Art. 57 UNCAC requires the Government to always return all assets subject to forfeiture to the State where the offence was committed. In general, during the period from 2016 to 2020 in the scope of 66 foreign cases around EUR 149.5 million in total was frozen. As per the assets forfeited, during the same period in the scope of 33 foreign cases EUR 58 million was forfeited of which in 21 cases there was an enforcement of foreign court order, and 12 cases resulted in repatriation without a forfeiture order. Only in 2 cases the request for enforcement of around EUR 14.2 million was refused (see IO.8), whereas in both cases the involved amounts are still frozen.

Extradition

715. No specific prioritisation criteria and request processing deadlines are developed for examining extradition requests. As described under R.39 extradition proceedings are initiated either by the execution of an internationally disseminated arrest warrant by the police, or through a request for extradition, which leads to the examination of the admissibility of the request and of a national arrest warrant. In both cases, it is necessary that a formal extradition request is submitted, together with a valid arrest warrant, the relevant facts and the applicable penal provisions. If the conditions for arrest are met, the arrest is executed (see R.39). Extradition to neighbouring countries takes place at the border with Switzerland or Austria, and sometimes Germany. In case of an extradition request of a non-neighbour-state the person to be extradited is transferred to the Zurich Airport. A transit permission of the Federal Office of Justice in Bern is necessary and is applied for by the Office of Justice without a formal MLA request.

Table 8.3: Incoming Extradition Requests – Offences the subject of requests

	2016		2017		2018		2019		2020	
Offence	rec.	exec.	rec.	exec.	rec.	exec.	rec.	exec.	rec.	exec.
ML	1	1	-	-	-	-	1	1	-	-
Fraud	2	2	-	-	1	1	-	-	1	1
Tax fraud	-	-	-	-	1	1	-	-	-	-
Drug trafficking	-	-	1	1	-	-	1	1	-	-
Robbery or theft	1	1	1	1	8	7	3	3	2	2
Execution ~		***100%***		***100%***		***87.5%***		***100%***		***100%***

716. Overall, during the period under review the country has received 26 extradition requests 21 have been executed, 5 are pending and 1 request has been rejected. In this specific case

extradition permission was rejected by another country which had initially extradited the person to Liechtenstein. Most of the incoming requests were related to robbery and theft, followed by fraud. No terrorism or TF related requests were received. Most of the requests come from neighbouring countries.

717. The average time taken for conduction of extradition was 2016- 41 days, 2017-71 days, 2018- 156 days, 2019- 158 days, 2020- 32 days respectively. The reason for the extradition being conducted in longer terms for some cases is the right of the persons affected to appeal the decision of the Court of Appeal to the Supreme Court and in some cases to the Constitutional Court.

Case Study 1- Extradition request on ML
In 2016 there was an extradition case with country A on ML, with the predicate offence being fraud. An arrest warrant against the country A national was issued by Country A court. In November 2017 this perpetrator was arrested in Liechtenstein due to a valid international arrest warrant. Afterwards, the Court of Appeal ordered his extradition. The person to be extradited appealed against his extradition to the Supreme Court but was not successful. All legal remedies in this extradition proceeding have been lodged and it took 215 days to surrender the person to the requesting state.

Case Study 2- Extradition request on Tax fraud
In 2018 Country B requested the extradition of a country B national because of tax evasion/VAT fraud. This person was sentenced to 6,5 years imprisonment by country B court. Due to the extradition request for the execution of the penalty the offender was arrested in Liechtenstein in July 2018. Legal remedies to the Supreme Court and the Constitutional Court were lodged but not successfully. The person was extradited within three months from the beginning of the extradition proceedings.

718. Overall, the country has demonstrated very high rates of execution of foreign extradition requests and the ability to provide timely and constructive extradition despite the absence of formal procedures in this regard. This was also confirmed by the Global Network.

8.2.2. Seeking timely legal assistance to pursue domestic ML, associated predicates and TF cases with transnational elements

719. Due to the Liechtenstein financial sector's exposure to predominantly foreign offences international cooperation plays an important role in countering criminality, thus the number of requests made to foreign counterparts is rather high. As further described under IO.7 most of the domestic investigations include foreign elements, thus the majority of investigations carried out by the Liechtenstein law enforcement authorities are accompanied with international cooperation requests (mostly outgoing).

720. Outgoing MLA requests are in practice prioritised in the same way as incoming ones. The judges responsible for passive MLA are also the ones in charge of dealing with active MLA. They ensure that the request is well made and adequately supported by documentation: the facts of the case corresponding to the requested measure and law are well set out. The contact details of the judge making the request are given, should there be a need to supply additional information. The authority for making MLA requests is adequately resourced. Requests are forwarded from the Court to the Office of Justice unless there is the possibility of direct transmission due to a bilateral MLA treaty (in which case, the Office of Justice also receives copies of such requests). The MLA request is registered in the database of the Office of Justice. After a review by the Office of Justice to verify the translation and ensure that the formalities are met the request is sent to

the central authority of the requested state within one or two days after receipt via the competent central authority or via diplomatic channel.

721. ML offences are the primary subject of the outgoing MLA requests. The remainder of the requests are related to other financial crimes, including fraud, insider trading and robbery and theft. Several requests have also been sent on corruption.

Table 8.4: Outgoing MLA – Offences the subject of MLA requests

Crime	2016	2017	2018	2019	2020	*Total per crime*
ML	144	145	179	225	173	***866***
Fraud, embezzlement, breach of trust	43	31	48	100	124	***346***
Corruption and bribery	0	2	0	0	0	***2***
Tax offences[35]	0	0	0	0	0	0
Narcotics	0	0	3	7	4	***14***
Theft and robbery	9	11	11	18	8	***57***
Insider dealing	7	3	6	9	5	***30***
Total per year	***203***	***192***	***247***	***359***	***314***	

722. Over the review period only one ML related MLA request has been refused on the ground of attorney-client privilege and no conflict of jurisdiction has been encountered. The average time taken to receive responses was: 2016- 117 days, 2017- 192 days, 2018- 112 days, 2019- 79 days, 2020- 159 days respectively. Usually, as explained by authorities they follow their internal deadlines and whenever a response is not received within 3-4 months, they reach back out the counterpart to follow up on the request. The authorities advised that they are generally satisfied with the quality of cooperation, however expressed concerns as per some countries, which usually do not provide responses for longer time periods. By the end of the onsite visit the country had 171 pending requests sent to foreign counterparts. As analysed under IO.6 and IO.7, this creates difficulties in obtaining evidence and thus making effective use of financial intelligence in national investigations.

723. As regards the types of measures requested from foreign counterparts, this extends to a broad range of international cooperation requests, including, but not limited to the types presented in the table below.

Table 8.5: Outgoing MLA- measures requested

Year	Interrogation	Seizure	freezing	Other (no coercive measures)
2016	24	9	1	170
2017	33	17	0	151
2018	25	21	2	205

[35] Tax offences committed abroad and follow up investigations are included into ML statistics. So far there have been 14 investigations where foreign tax offences were predicates with 18 MLA requests sent on these measures.

2019	64	66	6	261
2020	48	71	18	221

724. As discussed earlier and under IO.7 (also through case examples), Liechtenstein domestic investigations in relation to proceeds of crime generated outside of Liechtenstein, which have been laundered in or through the country very often lead to MLA requests to foreign counterparts in line with the threats faced by the country as an IFC.

Case Study 1- Outgoing MLA on self-laundering

Based on a complaint filed by a client against a Liechtenstein bank the OPP opened an investigation against unknown perpetrators for suspicion of fraudulent misuse of data processing and self-ML. Several banks in Liechtenstein and abroad were requested to surrender account and banking information. It was detected that the defendant abused the online banking system of the bank and caused a damage of more than EUR 1 million and that he laundered parts of the incriminated assets by purchasing gold, watches and jewels. Several MLA-requests were sent to 3 neighbouring countries requesting banks to surrender account and banking information and authorities to hear several witnesses. These requests were answered promptly, and the requested banking information and witness statements were transmitted. In July 2017 the OPP filed an indictment against the defendant charging him with fraudulent misuse of data processing and self-ML. Assets of the suspect in the amount of CHF 500 000 as property of corresponding value were forfeited, the suspect was sentenced to 33 months imprisonment.

Most of the requests were made to neighbouring countries, as well as United States, Canada, Italy, Albania, Macedonia, and Serbia. No statistics are available on the amounts involved in the MLA requests.

725. Regarding the extradition requests sent abroad, as in case of incoming requests there is no prioritisation criteria. The requests are sent through the Office of Justice following the same processes as in case of MLA requests.

Table 8.6: Outgoing extradition requests

	2016		2017		2018		2019		2020	
Offence	**sent**	**exec.**	**Sent**	**exec.**	**sent**	**exec.**	**Sent**	**exec.**	**Sent**	**exec.**
ML	1	1	2	2	4	4	3	3	3	3
Fraud	1	0	-	-	1	1	1	1	2	2
Drug trafficking	-	-	-	-	-	-	1	1	-	-
Robbery or theft	6	6	5	5	6	5	3	3	2	2
Total	**8**	**7**	**7**	**7**	**11**	**10**	**8**	**8**	**7**	**7**

726. During the period under review 41 extradition requests were sent to foreign counterparts, mainly to Switzerland, Germany and France. The underlying offences mainly related to ML, fraud, robbery, and theft. All the requests have been executed except for one, which was refused on the grounds on nationality and one, which is pending. There were no occasions for requesting extradition for TF.

8.2.3. Providing and seeking other forms of international cooperation for AML/CFT purposes

727. The competent authorities of Liechtenstein regularly seek other forms of international cooperation to exchange financial intelligence, supervisory, law enforcement or other information in an appropriate and timely manner with their foreign counterparts for AML/CFT purposes. This is done based on a number of international co-operation arrangements with other countries in the fields of financial intelligence, supervision and law enforcement (including bilateral and multilateral MOUs, treaties, co-operation based on reciprocity, or other co-operation mechanisms).

FIU

728. As described under IO.6 the FIU has the necessary powers to obtain and exchange with foreign counterparts a broad range of information, including administrative, financial and law enforcement information. The FIU plays an important role in international cooperation in Liechtenstein. It proactively and constructively cooperates with its foreign counterparts by exchanging information on ML, associated predicate offences and FT, which is evidenced by the positive feedback received from foreign counterparts, as well as the growing number of spontaneous disseminations sent abroad by the FIU (see Table below). Exchange of information is carried out both on the basis of a MOUs and based on the principle of reciprocity with the members of the Egmont Group via the ESW. To date the FIU has signed 26 MOUs, although this is not required for the exchange of information.

729. The information provided by the FIU to the foreign counterparts may be used as intelligence only. Before disseminating information along with its financial analysis to the domestic competent authorities (usually, to the OPP), the FIU obtains the consent from the foreign FIU. If this is not obtained, no dissemination is conducted. To date, there have been no confidentiality breaches nor have any concerns been expressed by the FIU's foreign counterparts in that regard. At the moment there are no undue limitations either under legislation or in practice, which would hinder the provision of international cooperation. It should be noted that starting from 2018 the FIUs powers have been increased by which it is not limited with an existing SAR/STR to make requests to persons subject to the DDA (see IO.6). Prior to the introduction of these legislative amendments the FIU could only provide assistance if there was a prior SAR/STR submitted domestically on the subject of the request. At the same time, it should be noted that no feedback was received from the global network related to limitations of effective cooperation between FIUs based on this ground. At that, the AT cannot assess whether the legislative provisions previously in force have in practice impacted effective cooperation and if yes, to what extent.

730. Based on the aforementioned legislative changes, together with the introduction of the regulatory framework for the VASPs sector, the number of outgoing spontaneous disseminations has been constantly growing resulting in the FIU more actively engaging in cooperation with foreign counterparts.

731. During the review period no TF related requests have been sent or received.

Table 8.7: Statistics on the international cooperation by the FIU

	2016	2017	2018	2019	2020
Requests for information sent by the FIU	308	235	165	184	271
Spontaneous disseminations sent by the FIU	N/A	N/A	53	109	803
Requests for information received by the FIU	269	204	145	163	156
Spontaneous disseminations received by the FIU	N/A	N/A	50	101	94
Average number of days to respond to requests	14	15	14	15	16

732. During the period under review, the FIU received a large number of foreign requests, a significant portion of which were from neighbouring countries. Responses were provided to all the requests. While responding to foreign requests, and in accordance with the internal procedures, the FIU not only uses information directly accessible to it, but also seeks additional information from national authorities and persons subject to the DDA. Authorities indicated that requests are responded to in average within 15 days, whereas the time limit for urgent requests is 5 days. Depending on the breadth and depth of an incoming request the FIU sets persons subject to the DDA a deadline of around 5 to 10 working days to reply to FIU requests in accordance with the requirement to respond to additional information under Art. 19a DDA when deemed necessary to fully respond to the incoming request. In some cases, a partial reply is sent immediately while additional checks are being carried out to fully respond at a later stage during the 10-15 working days period.

733. As regards the subject of the requests this usually entails administrative, financial and law enforcement information, such as: BO, financial flows, ownership and control of complex structures where one branch of the structure has been founded in or is managed by a Liechtenstein TCSP etc. With regard to the requests sent by the FIU those usually seek data and information on BO, source of funds and source of wealth, transactions, assistance for identifying additional accounts and/or natural/legal persons affiliated with mentioned/known subjects, law enforcement information (ongoing/finalized proceedings etc.). During the analysis of a case, when the FIU detects clear links with more than one country, if necessary, a specific request is sent to each foreign FIU for which the link has been identified. From 2018 to 2020 the FIU has opened 132 case files which had links to more than 2 foreign FIUs.

Case study- Cooperation on a case involving several FIUs
A client of a Liechtenstein TCSP holds a complex structure, with a Liechtenstein entity forming the top holding. Said client resides in country X and is a citizen of countries A and B. His main business interests are held in country C, while his assets are held with bank accounts in countries D, E and F. His family also holds real estate in countries A and C. Furthermore, from a transactional analysis the FIU has found indications that further business interests as well as close associates are also connected to country Y.

In this context, the FIU requested BO information and transactional history regarding known bank accounts; further information regarding potential (previously unknown) assets; general law enforcement information; presence of SARs/STRs; directorship of legal entities/arrangements in those jurisdictions; data from land register, car register, BO register, accounts register etc.

734. In general, the highest number of requests are sent and received from Switzerland, Germany, Russian Federation, Italy, United Kingdom, the Ukraine and the United States. Communication with foreign counterparts is carried out via Egmont Secure Web. In line with the EG Principles of Information Exchange, the FIU, to the largest extent possible, provides complete, factual and legal information, which includes the analysis of the case and its potential link with the requested country. This was also confirmed by the Global network which has also highlighted the development of the quality of communication received by the Liechtenstein FIU during the recent years. There have not been any cases of diagonal cooperation.

Police

735. The National Police actively cooperate with foreign counterparts in the framework of Interpol, Europol, as well as trilateral cooperation agreement with Switzerland and Austria. In 2011, the National Police established SIRENE office which provides access to Europe-wide searches for persons and property. It has its liaison officer with Europol, as well as maintains good cooperation with different liaison officers from FBI, DEA, etc. The National Police most frequently requests criminal records from abroad, as well as information regarding persons, companies (information on identity, place of residence, etc) and criminal investigations proceeding abroad. The requests received generally require clarifications on persons, companies, criminal intelligence, and national Liechtenstein findings.

Table 8.8: Statistics on international cooperation by the National Police

	2016		2017		2018		2019		2020	
Incoming requests	**ML**	**TF**	**ML**	**TF**	**ML**	**TF**	**ML**	**TF**	**ML**	**TF**
Received	123	3	64	2	87	4	118	3	166	5
Executed	123	3	64	2	87	4	118	3	166	5
Refused	0	0	0	0	0	0	0	0	0	0
average time of execution (days)	9	2	9	2	9	2	9	2	9	2
Outgoing requests	**ML**	**TF**	**ML**	**TF**	**ML**	**TF**	**ML**	**TF**	**ML**	**TF**
Sent	67	0	99	0	70	0	66	0	103	0
Executed	67	0	99	0	70	0	66	0	103	0
Refused	0	0	0	0	0	0	0	0	0	0

736. Upon receipt of a request, a case is opened if there is a connection to Liechtenstein and/or only such a connection from abroad is mentioned but not verified. After the case has been opened, information is gathered as a standard practice (requests to the FIU and to domestic/foreign authorities). The Criminal Investigation Division is informed about the request, which carries out a screening, to determine whether the FIU has already been informed. The Financial Crime Unit further clarifies whether the information gives rise to an initial suspicion of a domestic crime. If this is the case, the OPP is notified with a report.

737. The National Police advised that prioritisation and execution monitoring processes have been developed, however no formal documents on those processes were provided to the AT. In case the requests are marked as urgent they are dealt with as a priority. As regards the cases of

refusal to cooperate this normally includes the requests execution of which requires court order, thus this should be obtained through a formal MLA. An example of these requests is provision of banking information.

738. As regards the technical deficiencies identified under c.40.17 on providing stricter rules for the disclosure of information to foreign (non-EU) law enforcement authorities, it should be noted that the AT was presented with detailed statistics on cooperation of the National Police with a broad set of non-EU jurisdictions, thus demonstrating effective cooperation in practice.

739. The comments of delegations who shared their experience in police cooperation with Liechtenstein were generally positive, with some making reference to the excellent relationship between their own police forces and those of Liechtenstein. The country has also formed JITs, as well as engages in cooperation with Switzerland and Austria in the form of cross-border surveillance, controlled delivery, undercover investigations and joint observations. The last joint cooperation has been in 2019 with Switzerland while conducting a cross-border surveillance.

FMA

740. Banking, Insurance, Securities and DNFBP sector units of the FMA engage in cooperation with their foreign counterparts in relation to fit and properness, as well as market manipulation requests. The outgoing requests mainly relate to fitness and properness of management bodies as well as the shareholders of FIs or DNFBPs, including requests for a letter of good standing, information on previous convictions, insolvencies, defaults or other kinds of irregularities, AML compliance issues, etc.

741. During the period under review the outgoing requests made by the FMA mainly were related to the fit and properness of the banking, insurance, and securities sectors, while no request related to a TCSP was made (this is explained by the fact that Liechtenstein TCSPs very rarely have international subsidiaries or foreign shareholders/ managers).

Table 8.9: Outgoing Fit and Properness Requests

	2016	2017	2018	2019	2020	Total
Banking sector	5	9	11	10	12	**47**
Insurance sector	19	5	8	17	9	**58**
Securities sector	7	8	10	11	2	**38**

742. The requests were mainly made to Switzerland, Austria, Germany, Luxembourg, and United Kingdom. Several requests were also made to mainly other European countries. The geography, as well as the number of the outgoing requests is generally in line with the number of new applications, as well as their geographic presence.

743. It should also be noted that these requests are not only conducted at the licensing stage, when the applications are reviewed, but also after a licence has been granted. This is particularly the case if there are indications of a lack of guarantee of sound and proper business operation or if there are doubts about a person's fit and properness. The information requested mostly relates to supervisory findings on the part of the authority requested, such as information whether the person is suitable and provides financial soundness as requested by applicable regulation; confirmation that the person complies with the regulatory requirements and that the authority

requested is satisfied with the person's suitability and soundness; any special conditions imposed; proceedings in the past or currently pending.

Case Study- Outgoing fit and properness request
A foundation intended to acquire a qualified holding in a bank licensed under the Liechtenstein Banking Act. According to the information of the FMA the founder of the foundation was known to a supervisory authority of a third country. On March 10, 2020, the FMA sent a fit & proper request to the competent foreign supervisory authority and requested a set of information in relation to these entities and any actions taken against them.
According to the response of the supervisory authority of April 7, 2020 none of the entities in question nor the founder were under the supervision of the supervisory authority. Therefore, no non-public information regarding the entities and the founder was available. However, as one of the entities in question was operating in crypto-assets exchange services for residents without the necessary registration, the competent authority issued a warning notice with regard to this entity in 2018. The FMA was provided with an English translation of the notice. After issuing the warning notice in May 2018, the competent foreign supervisory authority has not taken any further supervisory measures or procedures with regard to this entity. The FMA, for its part, rejected the Foundation's acquisition of the qualified stake in the Liechtenstein bank.

744. As regards the cooperation with foreign counterparts prior to introduction of the VASP sector to the Liechtenstein market and granting licenses to the sector, one fit and properness request on VASPs has been made in 2020. Since 2018 the FMA has been cooperating with Germany, Switzerland and Austria to discuss and exchange experiences we each made in the VASP sector. Since 2019 the Regulatory Laboratory is also a member of the European Forum for Innovation Facilitators "EFIF" (https://esas-joint-committee.europa.eu/efif/efif-homepage),which provides a platform for supervisors to meet regularly to share experiences from engagement with firms through innovation facilitators, to share technological expertise, and to reach common views on the regulatory treatment of innovative products, services and business models, overall boosting bilateral and multilateral coordination. FinTech issues are also dealt with in the framework/different bodies of the European Supervisory Authorities (EBA/ESMA/EIPOPA). Various persons of the FMA are involved in this work. In relation to cooperation in the field of market abuse, Liechtenstein has sent a few requests for cooperation taking into account the absence of stock exchange in the country and subsequently absence of the need for cooperation in this field.

745. As per the incoming requests, about one third is related to fit and properness (including a few consolidated supervisions), and the rest is related to market abuse (requests under the IOSCO MOU).

Table 8.10: Incoming requests- Fit and properness and consolidated supervision

		2016	2017	2018	2019	2020	Total
Fit and properness	Banking sector	4	11	3	6	3	**27**
	Insurance sector	1	1	1	1	4	**8**
	Securities sector	-	-	-	-	5	**5**
	DNFBPs sector	4	2	19	2	4	**31**

Consolidated supervision	Banking sector	-	1	2	2	-	**5**
	Insurance sector	2	1	-	-	-	**3**

746. The requests mainly come from Switzerland, Austria, Germany, Malta, Hong Kong, Singapore, BVI and Cayman Islands in line with the geographic representation of these institutions. The information requested may be exchanged without any formal procedure. The processing of fitness & properness requests generally takes from 5 to 20 working days depending on the complexity of the request. Nonetheless, in some cases, especially related to banks' fit and properness requests it has taken from 46 to 85 days to fully respond to the request mainly due to several pending proceedings regarding the bank and its management bodies in question. There was an agreement between the FMA and the requesting authority to wait for further developments.

747. As per the requests related to market abuse, those are exclusively related to investigations or other inquiries in the area of securities supervision, most commonly in relation to insider trading and market manipulation coming from all over the world. These requests usually inquire account information, including KYC documents and the disclosure of the BOs. The provision of this kind of information is conducted upon approval by an Administrative Court through a special procedure. As regards the number of requests received, this constitutes 2016-45, 2017- 23, 2018-20, 2019-23, 2020- 21 respectively. It usually takes longer to respond to these requests due to the procedures in place for obtaining and sharing information. The authorities presented case examples to the AT confirming their successful cooperation with foreign counterparts in the framework of provision of information inter alia on BO.

748. While there are no prioritization criteria developed for the examination of incoming requests, all the incoming requests are dealt with as a matter of priority. In all divisions two officers per request are in charge of the processing of incoming requests in order to ensure the four-eyes principle. In case of absence of one of the persons responsible, deputy officers are in place.

749. During the period under review no requests have been denied. Between 2016 –2020 five fit & properness requests related to natural or legal persons not under the supervision of the FMA were received. The FMA could not issue a letter of good standing regarding those persons. No requests to conduct inquiries on behalf of foreign counterparts were made to the FMA. In the course of its activities the FMA has exchanged supervisory reports with its foreign counterparts and conducted joint inspections. An example of this activity is the joint supervision conducted together with the Italian supervisory authority from 2019 to 2021. Namely, Italian Supervisory authority *Istituto per la vigilanza sulle assicurazioni* (IVASS) conducted an AML/CFT on-site inspection at the Italian branch of a Liechtenstein insurance undertaking in which the FMA participated in the kick-off meeting and the final meeting. The results of this inspection in Italy were then taken into account by the FMAs own inspection at the head office of this insurance undertaking in Liechtenstein in 2021. In this inspection the IVASS participated as well and the results of the inspection thus were referred to IVASS.

Fiscal Authority

750. The Fiscal Authority is not entrusted with law enforcement powers and is not the competent authority regarding international co-operation for AML/CFT purposes. It does not handle requests from foreign AML/CFT authorities; however, the Fiscal Authority is the

competent authority for information requests regarding tax matters. when responding to a tax request the Fiscal Authority only corresponds with foreign tax authorities. Hence, even in cases where a tax request contains a ML element the Fiscal Authority does not directly correspond with foreign AML/CFT authorities. However, if the Fiscal Authority identifies a ML element in a tax request received from a foreign tax authority the Fiscal Authority reports the case to the Liechtenstein FIU. So far, no SARs/STRs have been filed with the FIU, however the authorities are in close contact, including discussions on individual cases. International cooperation is conducted in the framework of and in compliance with OECD Standards on EOIR and AEOI. Requests received in tax matters concern individuals in personal income tax matters as well as corporates in corporate tax matters. Regarding tax requests 14 requests have been denied (around 3% for reasons of e.g., tax period not covered by the agreement), while no requests have been sent.

8.2.4. International exchange of basic and beneficial ownership information of legal persons and arrangements

751. In general, the FIU, FMA and LEAs demonstrated to respond well to foreign requests for co-operation in respect of basic and BO information held on legal persons. This was also confirmed by the Global Network. The competent authorities in the field of cooperation on AML/CFT matters have the power to exchange basic and BO information. As provided under IO.5 the authorities rely on a range of measures to ensure BO information on legal persons and arrangements is available, primarily the newly introduced register of BO information, together with obligations on most legal persons to appoint a "qualified person" who is responsible for compliance with BO obligations. As provided under IO.5 all LEAs have sufficient access to adequate, accurate and current basic and BO information, this generally being obtained directly from FIs, DNFBPs and VASPs or legal person and arrangements through the LEAs, while the registers are used as a secondary source.

752. There is no statistical data available on the number of MLA requests sent to Liechtenstein asking for basic and/or BO information, as only the measures taken are recorded (e.g., based on Art. 96b CPC). However, the Liechtenstein law enforcement authorities ask the parties concerned (e.g. TCSPs or banks) for basic and BO information as a standard procedure. On the basis of MLA-requests law enforcement authorities are able to obtain all types of data and documents and information, in particular basic and BO information of legal persons and arrangements through a Court order. Usually, the investigating judge orders the institutions to provide the information and documents within 14 days, but in urgent cases the deadline may be shortened. The AT was presented with several case examples on successful exchange of information on BO information on the basis of MLA requests.

753. As regards the exchange of BO information by the FMA, it forms part of nearly each request related to fit and properness checks. Provision of such information has been demonstrated through case examples. BO information and information on banking account/business relationships is usually exchanged for the purpose of preliminary investigations of foreign authorities regarding potential insider dealings, market manipulation or similar securities related offences. In almost all of these requests, account information is requested with respect to individuals or legal entities, which typically includes the KYC documents and the disclosure of the BOs. During the period under review the FMA has exchanged 132 such information requests.

754. As per the FIU, exchange of BO information with its foreign counterparts takes place on a regular basis. As an FIU operating in an IFC and dealing predominantly with foreign UBOs, often also foreign legal entities and suspicions around predicate offences committed abroad the international exchange of information with foreign counterparts is very intense. A large no. of spontaneous information communications is sent out on a regular basis. This is especially the case when dealing with crypto related cases. It should however be noted that the same limitations described above have been in place regarding the ability of the FIU of obtaining information only based on a prior SAR/STR only. These limitations have been eliminated with the introduction of FIU broadened powers to exchange and request information irrespective of a presence of previous SAR/STR. On the other hand, no negative feedback has been received from the Global Network in this regard.

Overall conclusion on IO.2

755. Liechtenstein generally provides timely and constructive MLA, extradition and other forms of international cooperation, which was confirmed by the positive feedback from the global network. Competent authorities actively exchange basic and BO information on legal persons with their counterparts. During the period under review important legislative amendments were introduced in relation to provision of MLA on tax fraud, as well as removal of limitation of cooperation in the absence of a prior SAR/STR for the FIU further guaranteeing effective cooperation.

756. Issues were identified in relation to the risk of tipping-off as a result of the constitutional right of the entitled parties to be heard before the court prior to the execution of an incoming MLA and dual criminality requirement in relation to tax offences not criminalized in Liechtenstein. However, the country has taken mitigating measures in relation to these matters, although these could still have an impact on the effective cooperation. The AT, nonetheless, did not observe that this has been the case so far.

757. Overall, the AT is of the view that Liechtenstein has achieved the immediate outcome to a large extent, this being also confirmed by the positive feedback of the global network.

758. **Liechtenstein is rated as having a substantial level of effectiveness for IO.2.**

TECHNICAL COMPLIANCE ANNEX

This annex provides detailed analysis of the level of compliance with FATF 40 Recommendations in numerical order. It does not include descriptive text on the country situation or risks and is limited to the analysis of technical criteria for each Recommendation. It should be read in conjunction with the Mutual Evaluation Report.

Where both the FATF requirements and national laws or regulations remain the same, this report refers to analysis conducted as part of the previous Mutual Evaluation in 2014. This report is available from https://rm.coe.int/report-on-fourth-assessment-visit-anti-money-laundering-and-combating-/1680716b84.

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, they were not assessed under the 2014 mutual evaluation of Liechtenstein.

Criterion 1.1 – Liechtenstein completed its first National Risk Assessment (NRA I) in 2016. The assessment was carried out on the basis of the World Bank Methodology.

The second restatement of NRA I (NRA II) covering the period from 2016 to 2018 is composed of three parts: assessments of ML and on TF (both adopted by the Government in July 2020) and VAs (adopted in January 2020 and updated in August 2021).

The TF analysis is complemented by a TF assessment of the non-profit organisations (NPO) sector, which was finalised in May 2020[36].

In the course of the NRA II, the authorities were able, on the basis of experience gained in the course of NRA I, to collect a larger amount of data and statistics.

In the NRA II, the authorities have primarily used the FATF's National Money Laundering and Terrorist Financing Risk Assessment Guidance, while also taking into consideration, to some extent, the WB Methodology (i.e., to determine the relevant set of data and statistics to serve as the basis for the analysis). NRA II takes into consideration the country's risk profile as an IFC and the assessment gives this factor a central role. It concludes that IFC status is, in fact, an additional risk factor. Furthermore, specific risk analysis has been conducted in relation to trust and company service providers. NRA II is well oriented to understanding the overall ML/TF risks the country faces.

To this end, a range of threats is taken into consideration (geographic exposure, recurrent predicates committed abroad and domestically, types of customer). Cross-border transactions ("in-flow/outflow") carried out to/from the country for the period 2016 to 2018 have been systematically considered.

The analysis of vulnerabilities is dealt together with the analysis of threats for each financial and other sector in scope. The analysis reflects the findings/conclusions of the supervisory activities, including also the supervisors' findings in relation to the suspicious transactions reporting by persons subject to the DDA (i.e., section "AML compliance" is included for each sector examined).

These findings have been used to evaluate the level of residual risks. However, especially in the VASP sector, the final residual risk levels appear to reflect more the expected capability of the

[36] The report was prepared under the auspices of STIFA, which is a division of the Office of Justice. The following authorities took part in the preparation of the report: the FIU, OPP, Court of Justice; FMA, Fiscal Authority.

regulatory framework to mitigate risks than actual level of application of preventive measures - as evaluated through supervisory activities. For the VASP sector, it is still premature to draw conclusions on the regulatory capability to automatically lower its vulnerability and consequently its residual risk level, due to its early stage of implementation. The AT considers that this may, to some extent, understate the assessment of vulnerabilities/residual risk.

The Liechtenstein Post AG, in its capacity as an agent of a foreign payment institution, has been regarded in the broader context of transfer of funds to and from Liechtenstein, in the analysis of the MSB sector, although in the TF NRA only.

Specific risk analysis has been conducted in the ML NRA with regard to trust and company service providers. Four land-based casinos, all licenced, were subject to the ML risk analysis. Risks of online gambling have not been assessed given the moratorium regarding licences until the end of 2023.

As regards other DNFPBs (DPMS, lawyers and law firms, and real estate agents), NRA II notes that the risk categorisation from NRA I has not changed. Based on the fact that medium-low or low residual risk for these sectors was identified in NRA I, no further assessment was considered necessary by the authorities.

The range of data used to conduct the ML NRA is broad and grounded, ranging from information from SARs/STRs, number of existing and new business relationships (relationships with PEPs included), geographical information of customers and BO, requests for MLA (incoming/outgoing), etc.

The TF NRA (May 2020) focuses on TF risks to ensure that the specific factors that characterize TF threats and vulnerabilities are considered separately from those related to ML.

TF NRA also encompasses and was carried out on the basis of a broad range of information and data (cross-border flows of funds, statistics on trade; SARs/STRs; money service business statistics; inherent risk data collected by the FMA; intelligence involving TF or terrorism from foreign counterparts; criminal investigations and prosecutions; requests for international cooperation; cash declaration information; analysis of the commercial register in relation to involved parties and statutory purposes of legal persons/arrangements; demographic and work permit statistics; and open-source information).

In the course of the NRA II, trade bodies and associations were involved in the post-drafting process, mainly through providing comments and feed-back on the main findings of the assessment. These were taken into consideration for the final version of the NRA II.

Finally, the analysis of the risks posed by Liechtenstein legal persons and legal arrangements in relation to ML has been conducted by the Office of Justice with the involvement of other relevant authorities[37].

Specific ML/TF risk analysis was also conducted with regard to VAs and was finalised in January 2020 (and subsequently updated in August 2021). The assessment was carried out in line with the FATF guidance, and it examines and evaluates ML/TF vulnerabilities, threats and risks associated with VA activities in Liechtenstein (see under R.15).

[37] Ministry for General Government Affairs and Finance, Ministry for Foreign Affairs, Justice and Culture, the FIU, the FMA, OPP, Court of Justice and Court of Appeal and the Fiscal Authority.

Criterion 1.2 – The Liechtenstein Government established an AML/CFT Coordination Group - PROTEGE WG - by decision of 15 January 2013 (Working Group on the Prevention of Money Laundering, Terrorist Financing and Proliferation).

In addition, Art. 29a of the DDA states that '*the authorities responsible for the drafting of the national risk assessment, in particular the Public Prosecution Service, the FMA, the FIU, the National Police and other authorities engaged in the prevention of money laundering, organised crime and terrorist financing, shall take appropriate measures to identify, assess, understand and reduce the risks of money laundering and terrorist financing existing in this connection. The risk assessment must be updated at regular intervals.'* Consequently, NRA II (in its three component parts) was developed by the authorities represented in the PROTEGE and as per DDA (Art. 29 a).

The group is in charge of coordinating all policy and risk related action in the context of AML/CFT. Permanent members of the group are the Ministry for General Government Affairs and Finance, the FMA, the FIU, the OPP, the Court of Justice, the National Police, the Fiscal Authority, the Office of Justice, and the Office for Foreign Affairs. Other such as the Chamber of Lawyers and Office of Economic Affairs are also invited to attend meetings.

Starting from 2019, the PROTEGE WG is chaired by the Ministry for General Government Affairs and Finance.

Criterion 1.3 - On the basis of Art. 29a (1) DDA, NRAs are to be updated regularly. The update to ML/TF NRA I started in 2019 (2016-2018 data and information) and NRA II was adopted in July 2020, whilst the VA NRA II (data and information updated as of November 2019) was finalized in July 2020 (and subsequently updated in August 2021).

The update of NRA II is already scheduled, and the authorities have started collecting relevant data and information.

Criterion 1.4 - Liechtenstein relies on regular meetings of the PROTEGE WG to share results of the NRA. Furthermore, the full NRA II versions (ML, TF and VASP components) have been distributed by the Government to the private sector via their respective professional associations. They were directly forwarded to all casinos and all VASPs registered with the FMA, and also to those which are in the process of registration, or which have already announced their application to get registered. The authorities advised that this was done based on Art. 29c DDA which says '*the supervisory authorities and the FIU shall immediately provide the persons subject to due diligence with appropriate information to assist them in their own assessment of the risk of money laundering and terrorist financing.'*

In addition to that, the Summary of the NRA II (ML and TF), "key elements of the NRA", was sent to all relevant associations for distribution to the private sector. For those sectors not represented by an own association (casinos, VASPs) the documents were provided to market participants. All FIs and DNFBPs are therefore in possession of a copy of the summary (key elements) as well as all three NRA parts (ML/TF/VA) and the country's AML/CFT Strategy (see below).

Criterion 1.5 – Art. 29b (3) of the DDA states that the NRA *forms the basis for the allocation and prioritisation of resources for the prevention of money laundering and terrorist financing and for ensuring that appropriate regulations are put in place to address the risks*.

On the basis of the NRA II, Liechtenstein developed and adopted an AML/CFT Strategy in July 2020. The strategy refers to a global preventative approach with four high level outcomes: (i) implementation of international AML/CFT related obligations and standards; (ii) risk-based focus to increase the effectiveness; (iii) effective prosecution of ML and TF; and (iv) further intensification of national and international cooperation.

On the basis of the strategy, the Government is obliged to adopt an Action Plan setting out timetables, the competent authorities, and resources.

The Action Plan was adopted by the Government and its last update was made in August 2021. The Action Plan measures reflect the conclusions of the NRA II in its three components. The authorities advised that the plan should assist authorities` own risk-based approach in allocation of resources and implementing measures to prevent and mitigate ML/TF related risks. As a matter of fact, a number of measures in the Plan refer to the NRA II and correspond to some of the risks identified. In addition, measures dealing with an increase of human and other resources (e.g., '*reconciliation of institutional, legal, and operational frameworks as well as AML/CFT objectives and activities of public authorities with the country's risk profile according to the results of NRA II'*), are also a part of the Plan – the authorities advised that different risk levels were a key factor when allocating administrative, human or financial resources into different public institutions.

The AT also noted tangible actions which further confirm that several measures identified in the Action Plan have been already implemented in line with risks identified in the NRA (i.e., reorganisation of the FMA, additional employee at the National Police and planned future increase on expected budget, additional prosecutor joining the OPP, identification of the forfeiture of assets in relation to predicate offences committed abroad as a top priority policy objective, etc.).

Criterion 1.6 – The FATF Recommendations do not apply in five cases.

Case 1 - The DDA is not applicable to FIs operating in the field of occupational old age, disability, and survivors' provision (exempted pension funds) (DDA, Art. 4). The authorities have prepared a risk assessment in this respect which highlights that employer and employee contributions to exempted pension funds are deducted from salaries and that payments generally occur only in the case of death, disability, or old age. The exemption is available only to vetted employers.

Case 2 - The following activities which are covered by the FATF definition of FI are also not subject to the DDA: (i) lending (own funds only); (ii) financial leasing; and (iii) issuing and managing paper-based means of payment. See also R.10 to R.12, R.15, R.18, R.19, R.26, R.27, andR.35. The following activities which are covered by the FATF definition of DNFBPs (as applied by R.22 and R.23) are not subject to the DDA: (i) lawyers, law firms and accountants preparing clients for transactions in respect of the creation, operation or management of legal persons or arrangements; (ii) notaries; and (iii) some nominee services related to listed companies (in line with EEA provisions). See also R.22, R.23, R.28 and R.35.

Case 3 - There is no requirement to identify BO or take reasonable measures to verify identity where units in some investment funds are held on behalf of subscribing third parties by banks, fund trading platforms or central securities depositories from jurisdictions with due diligence and record-keeping requirements and supervisory standards that meet the requirements of Directive (EU) 2015/849, where ML/TF risk is assessed as low. This exemption follows risk factor guidelines issued by the European Banking Authority. In addition, for particular types of client accounts operated by lawyers, the obligations to identify and verify BO are replaced with a declaration made by the client (DDO, Art. 22b (3) and (4)). See also c.10.5.

Case 4 - There are some cases where the BO of a customer need not be a natural person (DDO, Art. 3(2)(b) to (i). This applies in a case where a customer is a: (i) public administration or enterprise; (ii) FI or DNFBP that is regulated and supervised in line with the FATF Recommendations; (iii) occupational pension scheme (in Liechtenstein or Switzerland); or (iv) common benefit entity that serves the benefit of the general public. In all of these cases, except (iv), such customers have been identified by the FATF as examples of potentially lower risk situations. See also c.10.5.

Case 5 - In the case of a member of the board of a foundation, board of directors of an establishment (with a similar structure to a foundation) or trustee, a legal person can be deemed as a BO of the customer (DDO, Art. 3 (1) (b) (2)). See also c.10.11.

Cases 2 to 5 are not based on an *ex-ante* assessment of risk and the assessment team (AT) cannot confirm that such hypothesis indicates: (i) a proven low risk of ML/TF; (ii) that these occur in limited circumstances; or (iii) that the activity is carried out on occasional basis. However, it is noted that the scope of the exemption for case 3 has been narrowed (since September 2021) to exclude investment funds which serve "individual asset structuring", pointing to some form of risk assessment having been conducted.

Criterion 1.7 **–** (a) On the basis of the DDA, the following business relationships and transactions are always to be assumed at higher risk: those involving PEPs (DDA, Art. 11(4)), cross border correspondent banking relationships (DDA, Art. 11(5)), complex structures (DDA, Art. 11 (6)) or relationships or transactions involving states with strategic deficiencies (DDA, Art. 11a(1)).

The Government is also entrusted to provide, by ordinance, specific regulations concerning EDD for different categories of customers, products, services, transactions and delivery channels. The Government can also identify, by ordinance, states with strategic deficiencies additional to those identified on the basis of the EU Directive 2015/849 (DDA, Art. 11(7) and 11a(6)(a)).

(b) In addition, legislation requires individual risk assessments to address possible indicators of higher risk, including the results of the NRA (DDA, Art. 9a (2)). The DDA provides for EDD measures (DDA, Art. 11) to be applied by persons subject to the DDA on the basis of their respective risk assessment (DDA, Art. 9a).

Where, on the basis of individual risk assessments, the existence of higher risks has been established, FIs and DNFBPs shall apply EDD (DDA, Annex 2 Section B) to the business relationships and transactions identified in order to address or reduce the increased risk (DDA, Art. 11).

Reasons for application of SDD and EDD have to be maintained in due diligence files (DDA, Art. 20(2) and DDO, Art. 27(1) cbis)).

Criterion 1.8 - Persons subject to the DDA may apply SDD measures if business relationships or transactions are deemed to only have a low ML/TF risk (rather than lower – as required under the FATF Recommendations), on the basis of their own risk assessment (DDA, Art. 9a and 10 (1)).

Assessments by persons subject to the DDA need to be consistent with NRA findings. Pursuant to Art. 22b (6) DDO the application of SDD is prohibited if there are indicators for potential higher risks.

Indicators and factors conducive to the application of SDD are contained in Annex 1A of the DDA.

Simplified CDD is not mandatory for a reporting entity; before applying it, persons subject to the DDA are requested to: (i) satisfy themselves that the risk associated with the business relationship is low; and (ii) monitor the business relationship and transactions sufficiently in order to ensure that unusual or suspicious transactions can be detected (RBA guideline of the FMA, Art. 5.5) (see also c.10.18).

Reasons for application of SDD have to be maintained in the due diligence files (DDA, Art. 20 (2) and DDO, Art. 27(1) cbis)).

Criterion 1.9 - The FMA is responsible for AML/CFT supervision (DDA, Art. 23 (1) (a)) and is in charge of implementing and ensuring compliance with the regulatory framework that is applicable to FIs, VASPs and DNFBPs (including casinos) – with the exemption of lawyers and law firms which are supervised by the Liechtenstein Chamber of Lawyers.

Based on Art. 24(3) DDA, all supervisory authorities verify that persons subject to the DDA are applying a risk-based approach. When conducting inspections, supervisors assess the adequacy of the business risk assessment of a person subject to the DDA including the adequacy and implementation of measures to reduce those risks (DDA, Art. 9a (5)).

FMA published FMA-Guideline 2013/1 on the risk-based approach under DDA. This guideline is intended to support FIs and DNFBPs when implementing the risk-based approach in practice.

For TCSPs, life insurance undertakings and life insurance intermediaries, the FMA has – in consultation with the private sector – developed a "customer risk assessment tool" (CRA tool) in order to assess the risk pertaining to their business relationships and transactions along the requirements outlined in FMA-Guideline 2013/1.

Criterion 1.10 - Art. 9a of the DDA requires persons subject to the DDA to conduct a business risk assessment.

(a) and (c) Risk assessments must be documented (DDA, Art. 9a (3) and DDO, Art. 22a (2)). They should also be updated on a regular basis, at least once every three years, unless the risk situation has changed meantime. In the latter case, the relevant risk-changing incidents have to be updated ad hoc (DDO, Art. 22a).

(b) When carrying out their risk assessments, persons subject to the DDA must pay special attention to the factors indicated in Annexes 1 and 2 of the DDA, other possible indicators of a potentially lower or higher risk, as well as the results of the national risk analysis (DDA, Art.9a). The FMA-Guideline 2013/1 indicates that once the risk analysis has been carried out, the individual business relationships and transactions must then be classified according to the identified risks, so that it is clear to those in charge which measures are to be taken in each individual case.

Based on the risk analysis, suitable internal control and monitoring measures must also be defined to reduce these risks. The risk assessment and the measures to reduce the risk must be appropriate and proportionate to the nature and size of the person subject to the DDA (DDA, Art. 9a (6)).

(d) Risk assessments are to be made available to the supervisory authorities for supervisory purposes (DDA, Art. 9a (3)).

Criterion 1.11 – (a) FIs and DNFBPs must define effective internal controls and supervisory measures to reduce the risks identified on the basis of: (i) national; and (ii) individual business risk assessments (DDA, Art. 9a(5)).

Persons subject to the DDA shall identify appropriate, internal organisational functions (contact person for relevant supervisory authority, internal unit for compliance functions, investigating officers) (DDA, Art. 21 and 22).

Persons subject to the DDA are also obliged to issue internal instructions setting out how the obligations arising from the DDA and the DDO are to be met in practice and ensure that all employees involved in the business relationship are aware of them – the content of the internal instructions is specified in legislation and needs to be approved at executive level (DDO, Art. 31(2) and (3)).

(b) An investigating officer (internal auditor) is responsible for ensuring compliance with the DDA, DDO and internal instructions (DDO, Art. 35). This responsibility does not expressly extend to monitoring compliance with internal controls and supervisory measures.

(c) Persons subject to the DDA are required to determine when EDD is required, i.e., establish criteria to identify business relationships and transactions involving higher risks, in their internal

instructions and are requested to define measures to reduce ML/TF risks identified (DDA, Art. 9a (4) and (5)).

Criterion 1.12 - Simplified measures can only be applied in situations where FIs and DNFBPs have verified that risks associated with the business relationship or transaction are low (rather than lower – as required under the FATF Recommendations (DDA, Art. 10(2)). In addition, it is specified that SDD may be applied only if persons subject to the DAA have identified a low risk (rather than lower) and have ensured that the business relationship or transaction is indeed associated with a low risk (rather than lower) (RBA guideline of the FMA, Art. 5.5).

Pursuant to Art. 22b (6) DDO, the application of SDD is prohibited whenever there is a suspicion of ML/TF.

Weighting and Conclusion

All elements of this Recommendation, except one, are complied with or largely complied with. Under c.1.6, it is highlighted that there are exemptions to the application of CDD and record keeping requirements which are not based on a proven low risk. However, overall, this shortcoming is considered to be minor for the following reasons: (i) the most important and widely used exemption (case 3) is commonly found in other countries and is based on guidelines issued by the European Banking Authority; (ii) given the focus of the private sector, gaps in Liechtenstein's definition of "financial institution" (case 2) and exemption offered to the legal sector to operate client accounts (also case 3) are not considered to be material; (iii) gaps in the application of the FATF Recommendations to lawyers, law firms and accountants when preparing clients for certain transactions (also case 2) are not noteworthy since these activities are, in practice, carried out through regulated TCSPs; (iv) exemptions under case 4 are linked to lower risk situations; and (v) the circumstances in which a member of the management body of a foundation, establishment or trustee administered by a TCSP (case 5) would be regarded as the BO will be very limited.

R.1 is rated LC.

Recommendation 2 - National Cooperation and Coordination

In the 4th MER of 2014, Liechtenstein was rated LC on R.31.

The main issues identified were related to the financial secrecy provision affecting the effectiveness of domestic information exchange and the need for the enhancement of cooperation between the FMA and the FIU. In the course of the follow-up process, Liechtenstein has taken steps in order to address these issues. It should be also considered that requirements in Recommendation 2 have changed since the last MER.

Criterion 2.1 - Liechtenstein has committed to establish a close cooperation between all national authorities responsible for combating ML and TF. A "Whole of government approach" was declared by the recently approved National Strategy. As discussed under R.1, the National Strategy to fight ML, predicate offences to ML, organised crime and TF was adopted in 2020 and was followed by the adoption of an updated Action Plan. Prior to that, the former Action Plan was in force – it resulted from the analysis carried out within the framework of the first NRA finalised in 2016.

For the implementation of the Strategy to combat ML, predicate offences to ML, organised crime and TF, four strategic objectives have been defined (see also R.1).

The Action Plan is regularly updated, e.g., it was revised in December 2020 in order to take into consideration the results of the NPO Report and measures identified in the NPO Report were integrated in the Action Plan.

The Action Plan, last update of which was made in August 2021, identifies a set of measures, to be implemented by different authorities within the PROTEGE WG, in order to improve preventative and repressive actions in respect to ML/TF and PF.

Aim of the measures are twofold - to improve preventative and repressive components in the overall AML/CFT/CPF system. The AP is divided into three lines composed of (i) measures which are yet to be adopted; (ii) measures which implementation is in progress; and (iii) measures already implemented. It takes into consideration areas of risks identified on the basis of the NRA II (examples of which are: limiting risks and supervision of anonymity - enhancing decentralised business models in the VA area, continuation of comprehensive and data-based sector-specific risk analyses by the FMA, including assessment of the risks associated with customers, geographical exposure, products and services offered with a view to NRA III, etc.).

In order to verify the level of implementation of the Action Plan, the PROTEGE WG is requested to report annually to the Government. If new risks arise, the Government can extend the Plan.

Criterion 2.2 – In 2013, Liechtenstein created a permanent national inter-office working group on combating ML, TF and PF – PROTEGE WG. It is responsible for coordination and cooperation in the above-mentioned areas and comprises all relevant AML/CFT stakeholders[38]. Starting from 2019 it is chaired by the Ministry for General Government Affairs and Finance. The PROTEGE WG reports directly to the Prime Minister and the members of the Government on such matters.

The PROTEGE WG is responsible for the strategy implementation and has the power to propose policies, submit proposals and / or measures. It reports annually to the Government on progress made against the Strategy. It is also in charge of examining operational issues that may arise in the activities of national authorities.

From the operational point of view, the PROTEGE WG is expected to meet regularly (5 to 6 times/year) and has the possibility to convene ad hoc if necessity arises.

Criterion 2.3 – The PROTEGE WG coordinates AML/CFT policies and related issues, it meets regularly and on ad-hoc basis if need be. It is a key mechanism for cooperation, coordination, and information exchange with regard to implementation of the AML/CFT policies and activities.

Art. 36 of the DDA requires all competent authorities active in the field of AML/CFT to cooperate and exchange information and data needed to enforce the objectives of the DDA. This also includes specific requirements for the OPP and Courts to inform the supervisors and the FIU about ongoing criminal proceedings[39].

In addition, supervisory authorities are regularly informed by the Public Prosecutor's Office on initiation and discontinuation of penal proceedings related to alleged violations of DDA (Art. 36 (3) and Art. 30 (1) DDA).

---

[38] PROTEGE WG composition is provided under C.1.2. As a Division of the Ministry of Justice, STIFA is represented within the PROTEGE WG meetings. Currently, the head of the STIFA Division is a member of the PROTEGE WG.

[39] Furthermore, the provisions of Art. 25 of the National Administration Act oblige, in particular domestic administrative authorities and courts, to provide domestic administrative assistance. Art. 25 of the National Administration Act is the legal basis for any exchange of information within the framework of administrative cooperation and accordingly enables any mutual exchange of information for the performance of the respective sovereign tasks, such as spontaneous administrative assistance in the exchange of information necessary for the performance of the tasks of other offices/authorities (this Art. Is not provided. If provided, can support the analysis).

On the operational side, in July 2020, the FIU, the FMA, the Public Prosecutor`s Office, the National Police and the Court of Justice signed an MoU outlining responsibilities, expectations, processes to be applied and the use of intelligence in ML/TF cases.

In general, Liechtenstein declared domestic and cross border cooperation, coordination, and exchange of information as a policy objective.

Criterion 2.4 - A sub-group under the PROTEGE WG which deals with targeted financial sanctions is also in charge of countering proliferation of weapons of mass destruction. It is composed of the FIU, the FMA, the Office for Foreign Affairs, the Ministry for General Government and Finance as well as the Government Legal Services.

Similar to Art. 36 DDA described above, Art. 6 of the ISA stipulates that the competent authorities, especially the courts, the Office of Public Prosecutor, the FMA, the FIU, the National Police, and other competent authorities in the field of sanctions' implementation are required to cooperate. If, within the framework of their inspections, the supervisory authorities (FMA and the Chamber of Lawyers) identify violations of the provisions of the ISA, they must inform the competent executing[40] authorities without delay. Moreover, Art. 7 ISA provides for cooperation with foreign authorities and with the UN.

Criterion 2.5 - DDA (Art. 37 b) states that the competent authorities may process personal data, including personal data concerning criminal convictions and offences of persons falling within the scope of this Act or give instructions for such data to be processed, insofar as this is necessary for the performance of their duties under this Act.

As for the cooperation mechanism aimed at ensuring compatibility between AML/CFT rules and data protection/privacy rules, relevant provisions are incorporated in the national Data Protection Act (DPA), the General Data Protection Regulation (GDPR, Regulation (EU) 2016/679) and to the DDA (Art. 36 (1a)).

On the basis of Art. 4 DPA, the processing of data by any public body is permitted if that is necessary to perform the task for which the controller is responsible.

The DDA (Art. 36(1)) serves as the basis for cooperation between competent authorities and specifies that the exchange of information between domestic authorities is lawful. Data Protection Authority competencies are specified under Art. 15 DPA. One of these competencies is cooperation and provision of administrative assistance to the supervisory authorities to ensure the consistency of application and enforcement of the DPA and other data protection provisions (Art. 15 (1)(g) DPA).

The Data Protection Authority may also be invited to participate in meetings of the PROTEGE WG if a specific data protection topic is to be addressed. In addition, the Liechtenstein Data Protection Authority would, *ex officio*, provide its legal opinion if any amendments to the legislation concern data protection issues. This framework, in view of the assessment team, satisfies the requirements of C.2.5.

Weighting and Conclusion

R.2 is rated C.

[40] Authorities clarified that "executing" in this context is the FIU as the competent authority for implementing and enforcing TFS (ISA (Art.3) and the provisions in the relevant ordinances. See under R.7.2.

Recommendation 3 - Money laundering offence

In the 4th round of MER in 2014 substantial progress in bringing the ML offence in line with the Convention and FATF Recommendations was noticed. Nevertheless, Liechtenstein was rated partially compliant regarding the criminalisation of ML due to effectiveness issues (level of proof required to establish the predicate offence, only one conviction since 2007, no autonomous ML prosecution). Therefore, it was recommended to pursue proactively ML as an autonomous offence in order to create jurisprudence on the burden of proof to establish the predicate offence. Increasing the effectiveness of the repressive approach by attenuating the formal high level of proof by amending the list-based ML offence to an all-crimes offence was recommended. The 2018 Follow up report concluded that progress has been achieved by Liechtenstein on the implementation of the effectiveness concerns related to former R1. Three convictions in autonomous ML cases were achieved, and on-going legislative measures were reported to address the deficiency regarding the level of proof required for the predicate offence.

Criterion 3.1 – ML is criminalised based on the Vienna and Palermo Conventions (Art. 165 CC). Art. 165 CC covers the physical elements as stated in the Vienna and Palermo Convention, i.e., concealment (hiding), acquisition, possession, management and use (conversion, realisation or transfer). Although Art. 165 CC does not contain specific terminology on the mental element (*mens rea*), it is clear that at a minimum the "wilful" standard applies. In Liechtenstein criminal law (Art. 5 CC) there are three forms of "*mens rea*" characterising an offence "wilfully", "intentionally" or "knowingly". When a criminal provision does not specify the mental element required, such as in Art. 165 (1), (2) and (3) CC, the act is deemed "wilful", which is an even lower standard than the required "intention" according to the terminology used in the relevant Conventions (Liechtenstein MER 2014 page 50 [154]). Apart from that Art. 165 (2) CC applies if a person "knowingly" appropriates or takes into safekeeping asset components originating from a misdemeanour under Art. 140 of the Tax Act (tax fraud).

In line with Liechtenstein criminal legislation, a person acts (i) with intent if such person desires to bring about the facts corresponding to the legal elements of an offence (Art. 5 para 1 of the CC); (ii) intentionally (purposefully) if it is important for him to bring about the circumstance or result for which the law requires purposeful action (Art. 5 para 2 CC); (iii) wilfully if he seriously believes that such facts can be brought about and accepts that they will be brought about (Art. 5 para 1 CC); and (iv) knowingly if he not merely considers the circumstance or result for which the law requires knowledge to be possible, but rather considers its existence or occurrence to be certain (Art. 5 para 3 CC).

Criterion 3.2 – The predicate offences for ML under Art. 165 CC can be divided in two categories: all criminal offences punishable with more than one year imprisonment and a list of specified misdemeanours (amendment of Art. 165 CC; law gazette 2019 no. 122). Until 2016 only VAT fraud exceeding CHF 75 000 affecting the budget of the EU was a predicate offence for ML (Art. 165(3a) CC); other categories of serious tax crimes such as large and organised income tax fraud were not predicate offences to ML. Since the amendment of Art. 165 CC (law gazette 2015 no. 371) all categories of serious tax crimes (related to direct taxes or indirect taxes) are covered: misdemeanours in accordance with article 140 of the Tax Act (income tax fraud) and in accordance with articles 88 or 89 of the Value Added Tax Act.

Criterion 3.3 – As stated in c.3.2, Liechtenstein applies a combined approach, partly threshold, partly list based, whereas, besides a list of specified misdemeanours, all criminal offences punishable with more than one year imprisonment are designated predicate offences.

Criterion 3.4 – Authorities advised that according to Art. 165 (5) CC, the offence of ML extends to any type of property that directly or indirectly represents the proceeds of crime, including

property of corresponding value. In accordance with tax offences (article 140 of the Tax Act and articles 88 or 89 of the Value Added Tax Act) savings are explicitly included in the definition of asset components and thus objects to ML (amendment law gazette 2019 no. 122).

In Liechtenstein legislation there is no legal definition of the term "property". According to the explanatory notes to the introduction of Art. 165 CC (law gazette 1996 no. 64) "property" includes all tangible assets, whether movable (such as funds, jewellery, securities, etc.) or immovable (houses, estates). The prevailing doctrine in Liechtenstein indicates that the term "property" also includes some other tangible assets such as VAs, and other rights with an asset value. Although the authorities are of the opinion that the explanatory notes to the introduction of Art. 165 CC is broad enough to encompass also intangible assets, purely for technical compliance purposes the AT could not find any provision which would cover these assets.

Criterion 3.5 – When proving that property is the proceeds of crime, the legislation does not require that a person is convicted of a predicate offence or that the predicate offence was the subject of prior judicial proceedings. In the case of ML committed in the interest of a criminal organisation or of a terrorist group (Art. 165 (3) CC) it is sufficient to prove that the property laundered belongs to a criminal organisation or a terrorist group.

To confirm the afore-mentioned, Liechtenstein authorities provided two cases (no. 12/451 and no. 14/368) where convictions for third party ML were obtained. In these cases, there was no previous conviction for predicate offences. These cases serve as a basis for instituting a prevailing doctrine in Liechtenstein and that is that it is sufficient that the predicate offence(s) is established whilst no conviction for this/these predicate(s) is required for pursuing ML offence(s).

Criterion 3.6 – Liechtenstein's criminal law does not require that the predicate offence is committed domestically, provided that the offence (if committed abroad) would constitute a criminal offence under Liechtenstein law. In addition, Art. 65(3) CC stipulates the general principle that it is sufficient that the offence is punishable under Liechtenstein laws if there is no penal power at the place where the criminal act was committed. Even if the predicate offence is committed in Liechtenstein and the ML takes place abroad, this is explicitly covered by Art. 64(1)(9) CC.

Criterion 3.7 – Self-laundering in Liechtenstein is criminalised in all cases of ML (Art. 165 (1) and (2) CC).

Criterion 3.8 – Authorities advised that the intentional element of ML offences may be inferred from objective factual circumstances, which are very often important factors affecting the judge's assessment of evidence. The judge is fully sovereign in assessing the value of the evidence (Art. 205 CPC).

This principle is confirmed in the judgement of the Court of Justice (self-ML cases dated 12 June 2019 (09 KG.2019.13)). The court stated that the objective course of events (i.e., objective, factual circumstances) were sufficient to establish that the accused knew that the money originated from crime; the accused accepted this fact and proceeded with a laundering activity.

Furthermore, and in the context of this criterion, the authorities referred also to cases 12/451 and 14/368 discussed under C.3.5. In these cases, the intentional element of the ML offence has been inferred from objective, factual circumstances. The authorities further advised that this principle is well established and applied by the courts in all types of criminal proceedings.

Criterion 3.9 – Natural persons convicted for ML offences are subject to imprisonment of a term not exceeding three years (Art. 165 (1) and (3) CC) or two years (Art. 165(2) CC). If the ML offence involves proceeds exceeding CHF 75 000 or is committed by a member of a criminal group associated for the purpose of continuous ML, the penalty may be elevated to imprisonment of one

to ten years depending on the circumstances (amendment law gazette 2019 no. 122). Sanctions for natural persons appear proportionate and dissuasive.

Criterion 3.10 – Art. 74a to 74h CC provide for a general criminal liability of legal persons entered in the commercial register as well as foundations and associations not entered in the commercial register for all criminal offences in addition to and independent from the liability of the natural persons prosecuted for the same act.

Penalties for legal persons are fines that are calculated based on the seriousness of the offence, the revenue of the legal person or entity and a scale of daily rates (number of daily rates from 40 up to 180; daily rate at least CHF 100 and at most CHF 15 000 [Art. 74b CC]). Furthermore Art. 74d CC stipulates that the legal consequences also apply to a legal successor if the rights and obligations of the legal person or entity have been transferred to another association by way of universal succession.

The liability of the legal person and the criminal liability of the managing staff or employees for the same act is not exclusive of each other (Art. 74a (5) CC).

Criterion 3.11 – Liechtenstein law provides comprehensive ancillary offences to the offence of ML as stipulated in Art.12 and 15 CC. This includes attempt (as well as participation in any attempt; Art. 15 CC), abetting another person to commit the offence or contributing to its perpetration in any other way (Art. 12 CC).

Weighting and Conclusion

All criteria are met apart from C.3.4 where a minor shortcoming with regard to the definition of property is noted - the legislation does not explicitly cover intangible assets.

R.3 is rated LC.

Recommendation 4 - Confiscation and provisional measures

In the 4th round of MER in 2014 confiscation, freezing, and seizing of proceeds of crime was rated LC, advising on the one hand to extend Art. 98 CPC to all relevant categories, such as payment system providers, e-money institutions, insurance mediators and DNFBPs, and on the other hand to restrict the scope of legal privilege in respect of auditors. Freezing of funds used for TF was rated PC due to the lack of procedures for domestic designations and public guidance on the procedures for de-listing from Al-Qaeda and Taliban UN list as well as for the fact that the scope of application of ISA was restricted in relation to UN Res. 1373. Apart from that, concerns in respect of the effectiveness were raised.

Criterion 4.1 – According to Art. 19a, 20, 20b and 26 CC Liechtenstein has implemented measures providing for confiscation of all proceeds of crime, laundered property, instrumentalities of crime, property related to criminal activities committed within the context of a criminal or terrorist organisation, savings, and property of equivalent value, regardless of – except confiscation (Art. 19a CC) – whether the property is held by criminal defendants or third parties.

These measures apply as follows (CC as amended in 2015 (law gazette no. 161) and in 2019 (law gazette no. 124)):

• Confiscation (Art. 19a CC) covers instrumentalities, i.e., tangible "objects" that the perpetrator used, intended to use in a criminal act or which were obtained from a criminal act.

• Forfeiture (Art. 20 CC) covers all assets (also VAs) obtained for or through the commission of any criminal act. This includes ML, predicate offences, and TF. It also includes gross profits, benefits resulting from proceeds (e.g., interest gained), assets replacing the original proceeds and

assets of equivalent value. The monetary value of assets saved through committing a punishable act (savings) are also subject to forfeiture.

• Extended forfeiture (Art. 20b CC) covers assets at the disposal of a criminal organisation, terrorist group or assets that are provided or collected for the financing of terrorism (para 1). It also covers – with a rebuttable legal presumption – assets obtained in a temporal connection with other offences (para 2 and 3).

• Deprivation order (Art. 26 CC) allows confiscation of any objects (instrumentalities) used by the perpetrator or intended by the perpetrator to be used to commit the criminal act, or any objects obtained from this act, if these objects endanger the safety of persons, morality or the public order.

Thus:

a) Forfeiture (Art. 20 CC) and extended forfeiture (Art. 20b (3) CC) cover the confiscation of property laundered.

b) Forfeiture (Art. 20 CC), extended forfeiture (Art. 20b CC), confiscation (Art. 19a CC) and the deprivation order (Art. 26 CC) cover the confiscation of proceeds of, or instrumentalities used or intended for use in, ML or predicate offences.

c) Forfeiture (Art. 20 CC) and extended forfeiture (Art. 20b (1) and (3) CC) cover the confiscation of property that is the proceeds of, or used in, or intended or allocated for use in the financing of terrorism, terrorist acts or terrorist organisations.

d) Forfeiture (Art. 20 (3) CC) and extended forfeiture (Art. 20b (4) CC) cover the confiscation of property of corresponding value.

Criterion 4.2 – a) Liechtenstein LEAs are obliged to take appropriate investigative measures to identify, trace, freeze and initiate seizing of property subject to confiscation. The OPP and the National Police can initiate an investigation based on a simple suspicion raised by a variety of (even open) sources such as press articles, police intelligence/reports, FIU reports and foreign investigations. The National Police within their duty to investigate offences ex officio (Art. 9 and Art. 10 CPC) are responsible, while investigating an offence, if there is a suspicion that assets were obtained for or through the commission of an offence, or that objects were used in the commission of an intentional offence (instrumentalities), to carry out an investigation on forfeiture, extended forfeiture, a deprivation order or confiscation and to report these investigation results to the Public Prosecutor's Office.

In addition, the National Police are endowed with an independent power to seize objects (Art. 96a CPC). Art. 96a (1) CPC provides that the National Police are entitled to seize objects on their own initiative if these objects are not subject to anyone's power of disposal, if they were taken from the injured party through the offence, if they were found at the scene of the offence and might have been used to commit the offence or might have been intended for that purpose, or if they are of little value or can easily be replaced on a temporary basis, if the possession of such objects is generally prohibited, or if they are found on a person arrested by the National Police or found in a search that the National Police are permitted to carry out on their own accord. This independent power of seizure granted to the National Police only concerns objects and its primary purpose is thus to ensure a deprivation order or confiscation.

The authorities also advised that since April 2020 an anonymous whistleblowing system is operated by the National Police to combat ML and proceeds generating predicate offences. The whistle-blower system, introduced by a decision of the Government in 2019, is used in cases of ML, economic crimes, corruption offences and the financing of terrorism, thus the most common proceeds generating predicate offences. This system is also intended to detect incriminated assets.

The authorities further advised that the legal basis for identifying and tracing suspect assets is laid down essentially in Art. 92, 96, 96b, 97a, 105, and 108 CPC. While these articles cover evidence gathering procedure, article 96b also specifies that in case the business relationship was or is being used for the transaction of a pecuniary advantage that is subject to forfeiture (Art. 20 CC) or extended forfeiture, banks, investment firms, insurance companies, asset management companies, management companies and managers of alternative investment funds shall, upon court ruling, (i) disclose the name, other data known to them about the identity of the holder of a business relationship, and such person's address; (ii) disclose whether a suspect person maintains a business relationship connection with that institution, is a BO or authorized person of such business relationship and, to the extent this is the case, provide all information necessary to identify that business relationship and deliver all documentation concerning the identity of the holder of the business relationship and his power of disposal; (iii) surrender all documents and other material concerning the type and scope of the business relationship as well as business transactions and other business events related to such business relationship from a certain past or future period of time.

b) Property identified to be subject to confiscation may be seized. The seizure regime in Liechtenstein is incorporated in Art. 97a CPC (freezing of assets) and Art. 96b CPC (seizure of objects and documents) and is used either for evidentiary purposes or to ensure effective forfeiture/confiscation. Distinction is made between the freezing measure of Art. 97a CPC which relates to assets and seizure according to Art. 96 and 96b CPC relating to objects and documents. Freezing and seizure actions require the involvement of the investigating judge pursuant to Art. 92, 96, 96b and 97a CPC. Freezing and seizure takes the items and assets into judicial custody. Pursuant to Art. 96a CPC the National Police is entitled to seize objects on their own initiative.

c) The National Police are empowered to take steps to prevent actions that prejudice the country's ability to freeze or seize or recover property that is subject to confiscation, such as immobilize assets, documents, and objects as conservatory measure in order to prevent their disappearance (Art. 25, 25a, 25b and 25c National Police Act).

d) The OPP may have the National Police, or the investigating judge carry out provisional inquiries (investigations) in order to obtain the necessary reference points for initiating criminal proceedings (investigation pursuant to Art. 41 CPC or indictment) against a specific person (Art. 21a CPC). At the request of the OPP, the National Police and the investigating judge can take any investigative measure, i.e., parallel financial investigations, to identify, trace and evaluate property. The National Police has to carry out inquiries on its own initiative (Art. 9 to 11 CPC). If on the application of the Public Prosecutor the investigating judge decides by way of a ruling to initiate an investigation, she/he has to investigate the punishable acts on his own and without further applications of the Public Prosecutor (Art. 41 and 42 CPC).

Criterion 4.3 – The relevant provisions do not specify any condition as to the location, possession, or ownership of the assets subject to confiscation. In principle, it is irrelevant if they are in the hands of third persons or not.

The rights of *bona fide* third parties are protected under Art. 20a (1) and (2) CC, Art. 20c CC and Art. 26 (2) CC. No forfeiture in accordance with Art. 20 (2) and (3) CC of assets belonging to a third party shall be made if such third party acquired such assets without being aware of the punishable act (Art. 20a (1) and (2) CC). Art. 20c and 26 CC provide for abstention from forfeiture and a deprivation order if the object or asset is legitimately claimed by a person who has not participated in the offence or in the criminal organisation or in the terrorist group (Art. 20c CC) or for objects which are legitimately claimed by a person who has not participated in the offence, in which case they will only be confiscated if the person concerned does not guarantee that the objects will not be used to commit the offence (Art. 26 (2) CC).

Criterion 4.4 – Freezing and seizure measures bring the items and assets concerned into judicial custody. Items are stored at the Court of Justice or at the National Police; money and other objects of value (especially jewellery and watches) are stored in safes. For larger items storage rooms or areas (especially for cars) are rented. For immovable assets a managing mechanism is not required since only the judicial prohibition of the alienation, encumbrance or pledging of real estate or rights registered in the Land Register can be ordered (Art. 97a (1) (4) CPC). Therefore, the real estate under such order is still managed by the owner. Frozen assets are kept in bank accounts. The account holder needs the approval of the Court of Justice for any changes in the investment. The primary investment target of frozen assets is protecting the capital and generating a regular income. Once there is a confiscation or forfeiture decision from the Court of Justice objects or assets which have been seized or frozen will become property of the state.

Weighting and Conclusion

R.4 is rated C.

Recommendation 5 - Terrorist financing offence

In the 4th round of MER in 2014 Liechtenstein was rated LC which was a significant improvement from the rating PC in the 3rd round of MER in 2008, due to prior legislative changes in accordance with the standard. Penalties were recommended to be increased to enhance deterrent effect.

Criterion 5.1 – Liechtenstein criminalises TF in line with the TF Convention through Art. 278d CC and other parts of the CC (i.e., Art. 278b and 278c CC). Art. 278d replicates the language of Art. 2 of the TF Convention and criminalises an activity which would involve provision or collection of funds, directly or indirectly, unlawfully, and wilfully, with the intention that they should be used or in the knowledge that they are to be used, in full or in part, in order to carry any of the offences provided in treaties annexed to the Convention (see also EC 5.2). Furthermore, the offence covers any act which is capable of bringing about serious or enduring disruption of public life or serious damage to economic activity, intended to intimidate the population in a grave way, to coerce public authorities or an international organization into an act, acquiescence, or omission, or to seriously subvert or destroy the fundamental political, constitutional, economic, or social structures of a state or an international organization (Art. 278c to which Art. 278d makes a reference as an offence for which TF provisions apply).

Criterion 5.2 – a) The offence in accordance with Art. 278d (1) CC extends to every person that makes available or collects assets/funds with the intent to be used, even only in part, to commit air piracy or intentional endangerment of aviation safety; extortionate kidnapping or a threat thereof; violence/attacks against internationally protected persons; unlawful handling of nuclear material or creating danger by nuclear energy; violence/attacks against civil aviation; offences against a ship or fixed platform; use of explosives against the public; committing a punishable act intended to cause the death of or grievous bodily harm to a civilian or any other person not actively participating in the hostilities during an armed conflict if such act by its very nature or due to the circumstances is aimed at intimidating a section of the population or coercing the government or an international organisation to act in a certain way or to refrain from such action; any other offence set out in Art. 278c (1), an offence set out in Art. 278e, 278f or 278g or the recruitment of another person for the commission of a terrorist offence set out in Art. 278c (1) (1) to (9) or (10) (amendment law gazette 2019 no. 158). The offences referred above cover all acts which constitute an offence within the scope of and as defined in the treaties listed in the Annexed to the TF Convention of the UN.

The definition of assets/funds was analysed under R.3 – criterion 3.4 and the conclusion reached therein (i.e., shortcoming concerns a lack of inclusion of intangible assets) is also relevant for this criterion.

b) The same penalties apply for someone who collects or makes available assets for a person or a group (Art. 278b (3) CC) committing an act referred to in sub-paragraph 1 or participating in such a group as a member (Art. 278d (1)(2) CC). According to the explanatory notes of Art. 278d (1) (2) CC(law gazette 2009 no. 49; Report and Motion 2008 no.124,) the peculiarity of this regulation is that it is not required that the financer had the intend that the financed person/group commits a terrorist act (with the funds and other assets made available to him/them), but that it is sufficient if the intention is that the individual/group to whom the funds and other assets are made available is a terrorist/terrorist group and that this person/group uses these funds and other assets for 'non-terrorist' purpose.

Terrorist group is defined in Art. 278b (3) CC as an affiliation of more than two persons intended to exist for an extended period of time and aimed at committing one or more terrorist offences (Art. 278c CC) or TF (Art. 278d CC) by one or more of its members.

Criterion 5.2bis – The CC as amended (2016 and 2019 [law gazette 2016 no. 14 and 2019 no. 158]) includes criminalisation of the training for terrorist purposes (Art. 278e CC) as well as the criminalisation of instruction to cause the commission of a terrorist offence (278f CC) and of travel for terrorist purposes (278g CC).

Art. 278d CC includes financing the travel of individuals who travel to a state other than their states of residence or nationality for the purpose of perpetration, planning, preparation of or participation in terrorist acts or providing or receiving of terrorist training. Financing of travelling for terrorist purposes in particular (Art. 278g CC) is covered by Art. 278d (1) Z 1(i) CC. Pursuant to Art. 278g CC any person who travels to another country in order to commit an offence set out in Art. 278b, 278c, 278e or 278f CC is punished with imprisonment of six months to five years (amendment law gazette 2019 no. 158).

Criterion 5.3 – Art. 278d CC extends to any funds whether from a legitimate or illegitimate source. Whilst this piece of legislation falls short to provide a definition of assets, the previous evaluation, when examining this issue (former c.II.1 b), confirmed that a commentary to the CC provides that the term "Vermögenswerte" (funds/financial assets in German) is to be understood in a broad sense and covers legitimate as well as illegitimate funds, corporeal as well as incorporeal property, and all assets representing financial value, including claims and interests in such assets. On the other hand, the shortcoming noted under R.3 and criterion 3.4 (lack of coverage of intangible assets) is also applicable for TF.

Criterion 5.4 –Art. 278d CC, read in conjunction with its Explanatory Memorandum (pls see criterion 5.2), does not require that the assets were actually used to carry out or attempt a terrorist act or be linked to a specific terrorist act.

Criterion 5.5 – The intentional element of TF offences may be inferred from objective factual circumstances. Liechtenstein relies on the principle of free evaluation of evidence by the judiciary codified in Art. 205 CPC. The judge is fully free in assessing the value of the evidence which enables him to make such inference.

In the absence of prosecutions and convictions for TF there is no specific case law to confirm the application of the afore-mentioned principle in TF related proceedings. On the other hand, there is a case law for other criminal offences, some of which (for ML) are discussed under R.3 where this principle has been applied. The authorities confirmed that the principles discussed in these cases (i.e., inferring knowledge from objective, factual circumstances) is applied in all criminal proceedings, including also in a potential trial for TF.

Criterion 5.6 – Since the 4th round of MER in 2014 the available penalties for natural persons for all types of TF offences under Art. 287d (1) (1) and (2) CC have been doubled to (minimum) one year to (maximum) ten years of imprisonment (law gazette 2016 no. 161). These sanctions are proportionate and dissuasive.

Criterion 5.7 – As stated above (c.3.10) regarding legal persons Art. 74a CC provides for general criminal liability of legal persons entered in the commercial register and foundations and associations not entered in the commercial register for all criminal offences in addition to and independent from the liability of the natural persons prosecuted for the same act.

Penalties for legal persons are fines that are calculated based on the gravity of the offence, the revenue of the legal person or entity, and a scale of daily rates (number of daily rates from 40 to 180; daily rate at least CHF 100 up to CHF 15 000 (Art. 74b CC). These sanctions are proportionate and dissuasive. Criminal liability of legal persons does not preclude parallel civil or administrative liability. The liability of the legal person for the underlying act and the criminal liability of the managing staff or employees for the same act is not exclusive of each other (Art. 74a (5) CC). Furthermore Art. 74d CC stipulates that the legal consequences also apply to a legal successor, if the rights and obligations of the legal person or entity have been transferred to another association by way of universal succession.

Criterion 5.8 – Liechtenstein has implemented comprehensive ancillary offences to the offence of TF as stipulated in Art. 12 and Art. 15 CC. This includes attempt to commit TF (as well as participation in any attempt; Art. 15 CC), as well as abetting another person to commit the offence or contributing to its perpetration in any other way (Art. 12 CC). Organising or directing others to commit a TF offence and contributing to the commission of one or more TF offences by a group of persons, acting with a common purpose is covered through Art. 278b CC on terrorist groups (see definition under c.5.2; Art. 278b (3) CC). Any person who participates in a terrorist group as a member (Art. 278 (3) CC) or who supports the group financially, is punished with imprisonment of one to ten years (Art. 278b (2) CC). Contributing to the commission of these offences in any other way is also covered (Art. 12 CC).

Criterion 5.9 – All TF offences are predicate offences for ML.

Criterion 5.10 – As long as the financing activity takes place in Liechtenstein it is irrelevant where the person committing the offence is located or where the terrorist activity itself takes place (jurisdiction *ratione loci*). Liechtenstein explicitly claims jurisdiction over TF committed in another country when the conditions of Art. 64 (1) CC are met. The article states that the Liechtenstein criminal laws apply to the offences listed in paragraphs 1-5 when committed abroad, irrespective of the criminal laws of the place where the act is committed. Although paragraphs 1-5 do not specifically refer to the TF offence, paragraph 6 of the same article states that this principle should also be applied to 'all other offences prosecutable in Liechtenstein.

Weighting and Conclusion

The only shortcoming concerns the definition of property – details of which are also provided under R.3 – there is no explicit coverage of intangible assets in the legislation.

R5 is rated LC.

Recommendation 6 - Targeted financial sanctions related to terrorism and terrorist financing

Special Recommendation III was rated PC in the 2014 MER of the Liechtenstein. The report noted: (a) the restricted scope of application of ISA in relation to UNSCR 1373; (b) the absence of procedures in place for domestic designations; and (c) the absence of public guidance on the procedures for de-listing from the Al-Qaeda and Taliban UN list. Furthermore, effectiveness was affected by deficiencies in CDD application and transparency of legal persons and arrangements.

Criterion 6.1 – Liechtenstein implements targeted financial sanctions (TFS) pursuant to UNSCR 1267 and 1988 (on Afghanistan) and UNSCR 1267/1989 (on Al Qaeda) through the ISA. In line

with the Law, the Government has issued two Ordinances allowing for the implementation of the said UNSCRs (i.e., Ordinance of 4 October 2011 on Measures against Persons and Organisations associated with the Taliban, as amended in August 2021 (Taliban Ordinance); and the Ordinance of 4 October 2011 on Measures against Persons and Organisations associated with ISIL (Da'esh) and Al-Qaida, as amended in August 2021 (ISIL/Al-Qaida Ordinance).

(a) The Government has the authority to enact compulsory measures (ISA (Art. 2)). The Government and the administrative offices designated by the ordinances are the executing authorities (ISA (Art. 3)), entitled to cooperate with the UN in exchange the information, (ISA (Art. 7)) The ISA does not explicitly provide the power for proposing persons or entities to the 1267/1989 and the 1988 Committees for designation. Nonetheless, the Ordinances and the newly introduced Instructions on the procedure for requests for designation on a sanctions list or removal from a sanctions list (the Instruction) empowers the Office for Foreign Affairs to notify the competent committee of the UN Security Council of the proposal for designation on the UN list based on a Government decision.

(b) Liechtenstein has introduced mechanism(s) for identifying targets for designation, based on the designation criteria set out in the relevant UNSCRs through the ISA and the Ordinances. The Instruction provides, that the FIU consults with other competent bodies and authorities before making a decision to recommend a designation. The FIU, with the assistance of the Office for Foreign Affairs, can also obtain additional information from jurisdictions in which the persons, groups, undertakings, and organisations have their domicile/residence and/or nationality or with which the persons, groups, undertakings, and organisations are otherwise linked, in accordance with the specifications of the applicable UN Security Council resolutions and the guidelines of the relevant sanctions committees.

(c) As provided under the Instruction, persons, groups, undertakings, and organisations are proposed to be designated under the UN list if, at the time of the decision, there are reasonable grounds or a reasonable basis for a designation. A criminal investigation, indictment, or conviction is not a necessary condition for such designation.

(d) Based on the Instruction the proposal to designate will be submitted to the relevant committee by the Office for Foreign Affairs in accordance with applicable procedures and forms as adopted by the UNSC committees whenever necessary. The proposal must be submitted together with all relevant documentation in the required format. The proposal must also indicate whether the nominating country is to be named as the country submitting the request.

(e) Mechanisms and procedures in relation to the details to be provided in the proposal for designation under UNSCR 2368 are provided under the Instruction, which provides for a list of information which should be included in the FIU's substantiated recommendation to the Government for the purpose of (requesting) designation of persons, groups, undertakings, and organisations on the UN list.

Criterion 6.2 – Liechtenstein implements UNSCR 1373 through the ISA, the Terrorism Ordinance, and the Instruction.

(a) Liechtenstein Government is the responsible authority, upon proposal from the FIU, for designating persons or entities that meet specific criteria for designation, as set forth in UNSCR 1373 (Art. 2 (1) of the ISA, Art. 4 of the Terrorism Ordinance). The Instruction further provides that FIU recommendation may be done whenever put forward by its own motion or, after examining and giving effect to, if appropriate, the request of another country. The Terrorism Ordinance includes identification information for identifying targets for

designation is described under Art. 4 of the Terrorism Ordinance. All the relevant designation criteria set out in the relevant UNSCRs are met.

(b) The mechanism for identifying targets for designation, is n general provided under Art. 4 of the Terrorism Ordinance, whereby the FIU, in collaboration with other competent authorities, should examine the targets for designation and refer recommendations for listing to the Government. Art. 3 of the Terrorism Ordinance defines the designation criteria as set out under UNSCR 1373.

(c) According to the Terrorism Ordinance (Art. 4), the FIU is the competent authority to receive requests and to evaluate and review these requests on the basis of the information and documentation available and in consultation and collaboration with the relevant authorities and bodies. The ISA (Art. 6) provides for cooperation between Liechtenstein competent law enforcement authorities with foreign competent authorities to the extent necessary for the enforcement of the Act and the ordinances under Art. 2 paragraph 2, corresponding foreign regulations or those of the UN. As for the procedures concerning incoming requests, in assessing whether the requests are supported by reasonable grounds, or a reasonable basis, to suspect or believe that the proposed designee meets the criteria for designation in UNSCR 1373 this is generally provided under the Terrorism Ordinance. At that, the FIU is solely required to review such requests on the basis of the information and documentation available to it (Terrorism Ordinance (Art. 4)). The Instruction does not provide for the promptness of determination, except for the cases when a foreign request is received.

(d) Application of "evidentiary standard" of proof in compliance with UNSCR 1373 is stipulated under the Instruction. Proposals for designations shall be based on decisions of the competent domestic or foreign authorities or courts in connection with: (a) the initiation of an investigation or criminal prosecution for a terrorist act or for the attempt of committing, participating in, or facilitating a terrorist act; or (b) a conviction for punishable acts (Terrorism Ordinance (Art. 3(2))). This provision is not compliant with the requirements set under C.6.2(d).

(e) Based on Art. 7 of the ISA when requesting another country to give effect to the actions initiated under the freezing mechanisms, Liechtenstein authorities would provide as much identifying information, and specific information supporting the designation, as possible.

Criterion 6.3 –

(a) Art. 4 of the Terrorism Ordinance gives the FIU general powers to collect or solicit information to identify persons and entities that, based on reasonable grounds, or a reasonable basis to suspect or believe, meet the criteria for designation. Further domestic and international cooperation mechanisms are provided under ISA.

(b) As regards the requirement to operate *ex parte* against a person or entity who has been identified and whose (proposal for) designation is being considered this is done through the Instruction and the ISA. Section 1 of the Instruction stipulates that any assessment for designation (on a national, or a UN list) by the FIU or other domestic law enforcement authorities is carried out without notifying the persons, groups, undertakings, and organisations under assessment. Furthermore, Art. 5 of the ISA stipulates that the bodies responsible for execution of the ISA, as well as third parties called upon for assistance, are obliged to preserve official secrecy.

Criterion 6.4 – According to the ISA (Art. 14a (1)) the Government, by ordinance, provides for automatic adoption of the lists issued or updated by the UNSC or the competent committee of the UNSC. All ordinances based on the ISA that implement UNSC sanctions regimes include a provision on the automatic adoption of UNSC lists (article 7a ISIL/Al-Qaida Ordinance and article

7a Taliban Ordinance), thus ensuring implementation of TFS without delay. As for implementation of UNSCR 1373, the assets and economic resources are frozen immediately upon publication of the designation as part of the publication of the amendment to the Terrorism ordinance.

Criterion 6.5 **–**The applicable processes for the freezing of funds are provided under the ISA and the ordinances. The requirement for all natural and legal persons within the country to "freeze" (as defined in the FATF Glossary), without delay, the funds or other assets of designated persons and entities is generally provided under Liechtenstein legislation. In particular, the ISA (Art. 1(2)) and the corresponding ordinances (i.e., Art. 2 of the ISIL/Al-Qaida Ordinance, Art. 2 of the Taliban Ordinance and Art. 1 of the Terrorism Ordinance) require that funds or other assets of designated persons and entities are frozen. The obligation to freeze without delay is provided under the Instruction. The freezing of funds is defined as "the prevention of any act that enables the management or use of the funds, with the exception of normal administrative acts by banks and investment firms", while the freezing of economic resources is further defined as "the prevention of use of these resources for the acquisition of funds, goods or services, including the sale, rental or pledging of such resources". Additionally, according to Art. 5(3) ISIL/Al-Qaida Ordinance, Art. 5(3) Taliban Ordinance and Art. 4(3) Terrorism Ordinance the competent Liechtenstein authorities shall take measures necessary to freeze economic resources, such as by noting a prohibition of disposal in the Land Register or by attaching or sealing luxury goods.

(a) The obligation to freeze does not restrict the scope of persons required to implement it. Nonetheless, the ISA and the ordinances are silent on the obligation to freeze without a prior notice. Whereas the ISA Guidance provides that this should be done without prior notice to the affected parties, this may not be considered an enforceable mean. The freezing obligation takes effect as soon as a designation is added to the Annexes of the Ordinances, which automatically adopt the UNSC and domestic sanctions lists.

(b) The terms "funds" and "economic resources" are defined in Art. 3 ISIL/Al-Qaida Ordinance, Art. 3 Taliban Ordinance and Art. 2 Terrorism Ordinance. Economic Resources include "assets of any kind irrespective of whether they are tangible or intangible, movable or immovable, in particular real estate and luxury goods, *with the exception of funds*." Economic resources and funds, both as defined by the afore-mentioned Ordinances, cover all types of funds and other property, as well as funds or other property derived from or generated from assets. The ordinances stipulate that any funds and economic resources that are partly or entirely owned by or under the direct or indirect control of those listed in the annexes and - in the case of the ISIL/Al-Qaida Ordinance and Taliban Ordinance – of those acting on behalf or on instruction of those listed in the annexes are frozen. As for the freezing of funds and economic resources under UNSCR 1373, the Terrorism Ordinance (Art. 1(1)) stipulates that any funds and economic resources that are entirely or partly owned or controlled directly or indirectly by individuals and legal persons, groups and organisations are frozen. According to the Terrorism Ordinance, there is no direct obligation to freeze funds or other assets (i.e. in the terminology of Liechtenstein legislation 'economic resources') of persons and entities acting on behalf of, or at the direction of, designated persons or entities.

(c) The Taliban Ordinance and ISIL/Al-Qaida Ordinance Art. 2(2) prohibits the transfer of funds to the designated individuals and legal entities, groups, and organisations concerned by the freeze or to provide them with funds and economic resources in any other way, be it directly or indirectly. Although the Ordinances do not include explicit prohibition to provide financial services or services related to the designated natural and legal persons, such a prohibition follows implicitly from the freezing obligation that is imposed on any person offering such

services and the cases of exemption to be provided. The Terrorism Ordinance Art. 1(2)(b) explicitly prohibits to provide other financial services for the designated individuals, legal persons, groups, and organisations.

(d) Art. 3(2) ISA allows enforcement authorities to issue instructions (in the form of a Guideline) outlining the detailed interpretation of the legal provisions set out in the ISA. The ISA Guideline provides the FIs and other persons or entities, including DNFBPs with guidance concerning their obligations in taking action under freezing mechanisms. Persons subject to the DDA are informed about designations, de-listings, or other modifications of the lists or of the sanctions regimes by a newsletter, which is sent through the "goAML" reporting application maintained by the FIU. This newsletter is updated on a daily basis and ascertains that persons subject to the DDA receive the relevant information without delay. Furthermore, because of the automatic adoption of UN sanctions lists by law in Liechtenstein, persons subject to the DDA are obliged to keep themselves up to date about changes of UN sanctions lists (e.g., by checking the relevant UN websites).

(e) Anyone who is directly or indirectly affected by measures in accordance with ISA, must without delay report to the competent executing authorities (ISA Art. 2b (1). If the measures are related to freezing of funds or economic resources this should be reported to the FIU (Taliban Ordinance, ISIL/Al-Qaida Ordinance Art. 6 and Terrorism Ordinance Art. 5, including the names of the beneficiaries and the subject and value of the frozen funds and economic resources. Neither the law, nor the ordinances include any provision on the reporting obligation in relation to attempted transaction. There is a reference under the ISA Guidance that the reporting also extends to attempted transactions, however this may not be concerned as an enforceable mean. In addition, while the ordinances provide for the reporting obligation of known economic resources, this does not extend to the known funds (as provided earlier, the definition of economic resources excludes the funds).

(f) The rights of bona fide third parties are protected under the ISA. At that, anyone acting in good faith when implementing the obligations under the ISA and the relevant ordinances shall be exempt from any civil and criminal responsibility (ISA, Art. 2 (a)).

Criterion 6.6 –

(a) The Instruction provides for the procedure on the request for removal from the UN list to be submitted by the Government upon recommendation of the FIU. As regards the designations under UN lists, The Sanctions Committee of the Security Council provides for a delisting from the UN Sanctions List procedure, information on which is available at the website of the Office for Foreign Affairs. The FIU Guidance for the implementation of the ISA further provided the link for de-listing through the UN Ombudsman as for the UNSCR 1267/1989.

(b) The ISA (Art. 8a) provides for the right to appeal against the administrative and governmental decisions and orders. At that, natural and legal persons, groups, undertakings and organisations affected by a coercive measure under the UNSCR 1373 may submit to the Government a substantiated request to have their name removed from the annex of an ordinance or for non-application of the coercive measure. The Government should decide on the request. The rules under the National Administration Act apply in principle (Section B 4 ISA Guideline).

The Terrorism Ordinance (Art. 4) specifies the relevant authority and procedure for a de-listing. The FIU will accept substantiated request for de-listing and unfreeze funds according to Art. 8a of ISA. The FIU, in collaboration with law enforcement and supervisory authorities, reviews on the basis of the information and documentation available to it, whether a person,

group or organisation should be deleted from the domestic list because they no longer meet the criteria for designation. The FIU requests the Government to remove a person, group, or organisation from the national sanctions list: (a) if it is of the view that the conditions for designation are no longer met; (b) if a court has determined that the designated body should be removed from a sanctions list, or (c) if the person in question is deceased. According to authorities if a decision is made to de-list a person, group or organisation, their funds or other assets should unfreeze immediately except where freezing is based on other legal provisions like due to separate criminal proceedings in Liechtenstein (either initiated by the OPP or by foreign countries in a request for mutual legal assistance). The FIU Guidance for the implementation of the ISA further describes the procedures for de-listing domestically.

(c) The ISA (Art. 9) provides for appeal procedures against the administrative and governmental decisions and orders. "Decisions and decrees of the Government may be appealed by way of complaint to the Administrative Court within 14 days of service". There is also the fundamental right to directly address the Constitutional Court in place (Art. 15(3) Constitutional Court Act).

(d) and (e) The Office for Foreign Affairs informs on its website about international sanctions that are implemented by Liechtenstein and provides a link to the applicable de-listing procedures in cases of UNSC sanction regimes. With regard to designations pursuant to UNSCR 1988, including those of the Focal Point mechanism established under UNSCR 1730 and with respect to designations on the UNSCR 1267/1989 Sanctions List, the UN Ombudsperson, pursuant to UNSCRs 1904, 1989, and 2083 is mentioned to accept de-listing petitions. The FIU Guideline refers to the Focal Point information.

(f) According to ISA (Art. 8a (1)) natural and legal persons, groups, undertakings and organisations affected by a coercive measure may submit to the Government a sustained request e.g., for non-application of the coercive measure. Guidance on procedures is provided by the FIU ISA Guideline (Section B 1 (4) and C 4 (1) of the ISA Guideline). According to FIU Guidance p 1.4, the FIU will be contacted if there is no clarity upon verification that the person or entity involved is not a designated person or entity. As for the procedures of unfreezing the funds or other assets of persons or entities with the same or similar name as designated persons or entities, who are inadvertently affected by a freezing mechanism if the FIU decides to confirm the "false positive", the *ex lege* freezing no longer applies, unless the addressee files a complaint against this decision.

(g) Persons subject to the DDA are informed about de-listings or other modifications of the lists or of the sanctions regimes by a newsletter, which is sent through the "goAML" reporting application maintained by the FIU. This newsletter is updated on a daily basis and ascertains that persons subject to the DDA receive the relevant information. Furthermore, because of the automatic adoption of UN sanctions lists by law in Liechtenstein, persons subject to the DDA are obliged to keep themselves informed about changes of UN sanctions lists, e.g., by checking the relevant UN websites, and thus to implement the measures, be it a freezing or in case of a de-listing the unfreezing. The FIU Guideline on the implementation of ISA does not include provisions on the obligation of the persons subject to the DDA to respect the delisting or unfreezing actions.

Criterion 6.7 **–** The Government has the authority to stipulate exemptions to compulsory measures in order to i.a. support humanitarian activities (ISA, Art. 2). The exemptions are enacted in the relevant ordinances that implement sanctions regimes. According to the ISIL/Al-Qaida Ordinance (Art. 2),the Taliban Ordinance (Art. 2) and with regard to UNSCR 1373, the Terrorism Ordinance (Art. 1) the Government, following the reporting to the competent UNSC Committee in accordance with the Committee's procedures and in accordance with the relevant resolution,

should approve payments from frozen accounts, transfers of frozen assets, or the release of frozen economic resources as an exception to avoid hardship cases, fulfil existing agreements, fulfil claims that are the subject of an existing decision by a court, an administrative office, or a court of arbitration, pay reasonable fees and reimburse costs in connection with the rendering of legal services, pay fees or costs for services for the routine safekeeping or administration of frozen funds or economic resources, provide humanitarian aid, denuclearisation, or safeguard Liechtenstein interests. Applications to such effect are to be submitted to the FIU. Nonetheless the wording provided under ordinances does not seem to explicitly cover all UNSCRs resolutions 1718 and 2231 requirements including basic expenses, payment for foodstuffs, rent or mortgage and extraordinary expenses. No explicit procedures with regard to processing applications in relation to the UNSCR 1373 are in place, apart from the applications to be submitted to the FIU. Clarifications have been provided under the ISA Guidance in this regard, however those are not considered to be an enforceable mean.

Weighting and Conclusion

Liechtenstein implements TFS measures pursuant to the relevant UNSCRs without delay. Nonetheless, there is no explicit requirement to freeze funds and economic assets without prior notice. Some deficiencies are also in place with regard to the scope of funds to be frozen, reporting obligation in relation to attempted transaction, as well as the scope of exemptions to be applied. No guidance is provided to the persons subject to the DDA on their obligation to respect the de-listing or unfreezing actions.

R.6 is rated LC.

Recommendation 7 – Targeted financial sanctions related to proliferation

Requirements under the R.7 were first introduced in the FATF Recommendations in 2012, therefore Liechtenstein was not assessed in the 2014 MER against this recommendation. The ISA sets out the general framework for the implementation of PF-related TFS. The national legislation and mechanisms described in R.6 apply equally to the criteria under Recommendation 7.

Criterion 7.1 **–** UNSCR 1718 and successor Resolutions on the Democratic People's Republic of Korea (DPRK) are transposed into the Liechtenstein legal framework through the ISA and the Ordinance of 24 May 2016 on Measures against the Democratic People's Republic of Korea, as amended (DPRK Ordinance). UNSCR 2231 on Iran is transposed into the Liechtenstein legal framework through the ISA and the Ordinance of 19 January 2016 on Measures against the Islamic Republic of Iran, as amended (Iran Ordinance). The two Ordinances complement the requirements of ISA which (ISA, Art. 14a (1)) permits the Government to establish by ordinance the automatic adoption of the lists issued or updated by the UNSC or the competent committee of the UNSC. The UNSCR lists concerning individuals, enterprises, and organisations or economic resources shall be adopted automatically (Art. 23a of the DPRK Ordinance and Art. 14a of the Iran Ordinance), thus ensuring implementation of the UNSCRs without delay.

Criterion 7.2 **–** The applicable processes for the freezing of funds are provided under the ISA and the ordinances. The requirement for all natural and legal persons within the country to "freeze" (as defined in the FATF Glossary), without delay, the funds or other assets of designated persons and entities is generally provided under Liechtenstein legislation. In particular, the ISA (Art. 1(2)) and the corresponding ordinances (i.e., Art. 11 of the DPRK Ordinance, Art. 8 of the Iran Ordinance) require that funds or other assets of designated persons and entities are frozen. The freezing of funds is defined as "the prevention of any act that enables the management or use of the funds, with the exception of normal administrative acts by banks and investment firms", whereby the freezing of economic resources is defined as "the prevention of their use for the acquisition of funds, goods or services, including the sale, rental or pledging of such resources".

In addition, the competent Liechtenstein authorities shall take the measures necessary to freeze economic resources, such as by noting a prohibition of disposal in the Land Register or by attaching or sealing luxury goods (Art. 19 of DPRK Ordinance and Art. 13 of Iran Ordinance).

(a) The obligation to freeze does not restrict the scope of persons required to implement it. Nonetheless, the ISA and the ordinances are silent on the obligation to freeze without a prior notice. The freezing obligation takes effect as soon as a designation is added to the Annexes of the Ordinances, which automatically adopt the UNSCR sanctions lists. This is provided under ISA Guidance, which is however not considered an enforceable mean as provided under R.6.

(b) The terms "funds" and "economic resources" are defined in Art. 1 of the DPRK Ordinance and Art. 1 of Iran Ordinance. Economic Resources include "assets of any kind irrespective of whether they are tangible or intangible, movable or immovable, in particular real estate and luxury goods." These terms cover all types of funds and other property, as well as funds or other property derived from or generated by the latter. The ordinances stipulate that any funds and economic resources that are partly or entirely owned by or under the direct or indirect control of those listed in the annexes and of those acting on behalf or on instruction of those listed in the annexes are frozen. According to the ISA Guideline "Control" could include, inter alia being a beneficiary of the legal person or entity (including prospective and discretionary beneficiaries).

(c) DPRK Ordinance (Art. 11) and the Iran Ordinance (Art. 8) prohibit to transfer funds to the designated individuals, enterprises, and organisations or to provide them with funds and economic resources in any other way, be it directly or indirectly. Making funds or economic resources available to non-listed legal persons or entities which are owned or controlled by a listed person or entity will in principle be considered as making them indirectly available to the latter, unless it can be reasonably determined, on a case-by-case basis using a risk-based approach, taking into account the criteria that the funds or economic resources concerned will not be used by or be for the benefit of listed person or entity.

(d) The ISA Guideline provides guidance to FIs and other persons or entities, including DNFBPs on their obligations in taking action under freezing mechanisms. Persons subject to the DDA are informed about designations, de-listings, or other modifications of the lists or of the sanctions regimes by a newsletter which is sent through the "goAML" reporting application maintained by the FIU. This newsletter is updated on a daily basis and ascertains that persons subject to the DDA receive the relevant information without delay. Furthermore, because of the automatic adoption of UN sanctions lists by law in Liechtenstein, persons subject to the DDA are obliged to keep themselves informed about changes of UN sanctions lists, e.g., by checking the relevant UN websites.

(e) Anyone who is directly or indirectly affected by measures in accordance with ISA, must without delay report to the competent executing authorities (ISA, Art. 2b(1). If the measures are related to freezing of funds or economic resources this should be reported to the FIU (DPRK Ordinance (Art. 21 (1)) and the Iran Ordinance (Art. 9)), including the names of the beneficiaries and the subject and value of the frozen funds and economic resources. Neither the law, nor the ordinances include any provision on the reporting obligation in relation to attempted transaction. There is a reference under the ISA Guidance that the reporting also extends to attempted transactions, however this may not be concerned as an enforceable mean. In addition, while the ordinances provide for the reporting obligation of known economic resources, this does not extend to the known funds.

(f) The ISA (Art. 2a) provides that anyone acting in good faith when implementing the obligations under the ISA and the relevant ordinances shall be exempt from any civil and criminal responsibility.

Criterion 7.3 – The ISA (Art. 3) stipulates that enforcement authorities are the Government and the official bodies designated by it by ordinance. With regard to the freezing of funds and economic resources the FIU is the competent executing authority (Iran Ordinance (Art. 8 and 9) and 22 DPRK Ordinance, Art. 19, 21 and 22). The ISA (Art. 2b and 2c) sets out reporting and due diligence obligations for those affected by measures. Furthermore, the Iran and DPRK Ordinances include additional detailed provisions on reporting duties and due diligence (DPRK Ordinance (Art. 21 and 22), Iran Ordinance (Art. 9)).

The ISA (Art. 5a) stipulates that the FMA and the Liechtenstein Chamber of Lawyers are the supervisory authorities under the ISA and in accordance with the DDA (Art. 23(1)). The ISA (Art. 5b) defines the responsibilities and powers of the supervisory authorities and stipulates that they are responsible for monitoring compliance with the special obligations of those subject to due diligence. Failure to comply with the obligations set forth by ISA and the corresponding ordinances leads to administrative or criminal sanctions (articles 11- 13 ISA), including confiscation of property and assets, fines up to 200,000 francs or imprisonment up to six months, if the fine cannot be collected. The responsibility of legal persons is governed by the provisions of Art. 74a et seq. of the CC and the DDA applied *mutatis mutandis.*

Criterion 7.4 –

(a) The Sanctions Committee of the Security Council provides for a delisting from the UN Sanctions List procedure, information on which is available at the website of the Office for Foreign Affairs. The FIU Guidance for the implementation of the ISA provides additional guidance in this regard. Further procedures are provided under the Instruction as set forth under C.6.6.a.

(b) According to ISA (Art. 8a (1)) natural and legal persons, groups, undertakings, and organisations affected by a coercive measure may submit to the Government a sustained request e.g., for non-application of the coercive measure. Guidance on procedures is provided by the FIU ISA Guideline (Section B 1 (4) and C 4 (1) of the ISA Guideline). According to FIU Guidance p 1.4, the FIU will be contacted if there is no clarity upon verification that the person or entity involved is not a designated person or entity. ISA Guidance further provides the procedures of unfreezing the funds or other assets of persons or entities with the same or similar name as designated persons or entities, who are inadvertently affected by a freezing mechanism.

(c) The Government has the authority to stipulate exemptions from compulsory measures in order to i.a. support humanitarian activities (ISA, Art. 2). Exemptions are enacted in the relevant ordinances that implement sanctions regimes. Exemption conditions as set out in UNSCRs 1718 and 1737 are met by the relevant provisions in the DPRK Ordinance and Iran Ordinance. According to the DPRK Ordinance (Art. 11(5)) and the Iran Ordinance (Art. 8(3)) the Government may authorise payments from frozen accounts, transfers of frozen assets, or the release of frozen economic resources as an exception in order to: avoid hardship cases, fulfil existing agreements, fulfil claims that are the subject of an existing decision by a court, an administrative office, or a court of arbitration, pay reasonable fees and reimburse costs in connection with the rendering of legal services, pay fees or costs for services for the routine safekeeping or administration of frozen funds or economic resources, provide humanitarian aid, denuclearisation, or safeguard Liechtenstein interests. Applications to such effect are to be submitted to the FIU according to the DPRK Ordinance (Art. 11 (8)) and the Iran Ordinance

(Art. 8(5)). They are, if needed, forwarded to the UN in accordance with the requirements of the relevant resolution or the relevant UNSC committee, coordinated by the Office for Foreign Affairs. Nonetheless the wording provided under ordinances does not seem to explicitly cover all UNSCRs resolutions 1718 and 2231 requirements including basic expenses, payment for foodstuffs, rent or mortgage and extraordinary expenses. Clarifications have been provided under the ISA Guidance in this regard, however not being an enforceable mean.

(d) Persons subject to the DDA are informed about de-listings or other modifications of the lists or of the sanctions' regimes by a newsletter, which is sent through the "goAML" reporting application maintained by the FIU. This newsletter is updated on a daily basis and ascertains that persons subject to the DDA receive the relevant information. Furthermore, because of the automatic adoption of UN sanctions lists by law in Liechtenstein, persons subject to the DDA are obliged to keep themselves informed about changes of UN sanctions lists, e.g., by checking the relevant UN websites, and thus to implement the measures, be it a freezing or in case of a de-listing the unfreezing. The FIU Guideline on the implementation of ISA does not provide for a provision on the obligation of persons subject to the DDA to respect delisting or unfreezing actions.

Criterion 7.5 –

(a) While interests or other earnings can be subsumed as "funds" as defined in the DPRK Ordinance (Art. 1) and the Iran Ordinance (Art. 1), no explicit provision is in place to permit the addition to the accounts frozen pursuant to UNSCRs 1718 or 2231 of interests or other earnings 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 any such interest, other earnings and payments continue to be subject to these provisions and are frozen.

(b) According to the Iran Ordinance (Art. 8(3)) the Government authorises exemptions in accordance with the relevant UNSC resolutions, if these are applicable, and may approve payments from frozen accounts for i.e., the fulfilment of existing agreements. Applications to such effect are to be submitted to the FIU according to Iran Ordinance (Art. 8(5)). They are, if needed, forwarded to the UN in accordance with the requirements of the resolution or the relevant UNSC committee, coordinated by the Office for Foreign Affairs.

Weighting and Conclusion

Liechtenstein implements the PF related TFS without delay under its national legal framework pursuant to the relevant UNSCRs. However, there still remain some deficiencies, in particular in relation to the scope of funds covered by the freezing obligation, the reporting requirement noting extending to attempted transaction, no clear provisions on permitting additions to accounts. No guidance is provided to the persons subject to the DDA on their obligation to respect the de-listing or unfreezing actions.

R7 is rated LC

Recommendation 8 – Non-profit organisations

Special Recommendation VIII was rated PC in the 2014 MER of the Liechtenstein. There was no review to understand the activities, size, and other relevant features of NPOs in Liechtenstein in order to determine the features and types of organisations that are at risk of being misused for FT. In addition, there was no periodic re-assessment by reviewing new information on the sector's potential vulnerabilities to terrorist activities and not all common-benefit entities are subject to supervision. No measures were in place to sanction violations of oversight measures or rules by NPOs or persons acting on their behalf.

Criterion 8.1 –

(a) An analysis of the NPO sector was conducted under the direction of STIFA in cooperation with the FIU, FMA, Fiscal Authority, Court of Justice and the OPP in 2019-2020 (NPO Risk Report) with the purpose of identifying those legal entities that fall within the functional FATF definition of NPOs and are at most risk of abuse for TF purposes (see IO.10). The NPO Report identified 52 high-risk NPOs, mainly common benefit foundations and establishments, with the residual medium-low TF risk, while the common-benefit associations were assessed to be at low risk of TF. The total number of high-risk NPOs has increased to 53 as per June 2021. NPOs identified as "high-risk" represent only a very small proportion (3.6 %) of the total NPO sector.

(b) Based on the Characteristics of NPOs at risk, the NPO Risk Report identified the threats posed by terrorist entities to the entire NPO sector, including potential scenarios of TF abuse. Concerning the TF abuse, it is particularly conceivable that domestic NPOs fall into the clutches of foreign organisations acting from abroad under the guise of a sham NPO, or that they could become the victim of false representations by terrorist organisations. Some common-benefit foundations and common-benefit establishments manage substantial volumes of assets and therefore may handle a larger number of financial transactions. Associations do not administer high volumes of assets and usually do not show any international presence. The same scenarios may also apply to associations qualified as NPO, whereby here, other than with foundations and establishments, the registration of sham associations in Liechtenstein cannot be excluded due to the comparatively reduced requirements (NPO Risk Report, May 2020, Sections 5 and 7).

(c) The NPO Risk Report analyses existing risk mitigating measures, including the adequacy of the legal and institutional framework in place. At that, common-benefit foundations and establishments are subject to several of risk-mitigating measures, including registration and supervision, as well as record-keeping and due diligence requirements. The due diligence requirements apply to the qualified member of the administrative body and that, in this respect, supervision by the FMA of common-benefit foundations and establishments is carried out (indirectly) via the qualified member of the administrative body (TCSP). The Liechtenstein legislation does not impose similar requirements in relation to associations, however, those associations falling under the FATF definition of NPOs have in practice registered with the commercial register and the Fiscal Authority. The NPO Risk Report concludes that (a) it should be examined whether a mandatory appointment of a qualified administrative body under Art. 180a PGR would be appropriate for those associations falling under the FATF's definition of NPOs; (b) it should be examined to what extent the exchange with representatives of the association sector can be improved in future, in particular to ensure the necessary raising of awareness.

(d) The 2019-2020 NPO report was the first analysis of the sector, while an update of the NPO Risk Report will be conducted in 2022 as stated in the report. No specific periodicity of review of the NPO sector is further specified.

Criterion 8.2 –

(a) A number of measures intended to promote the accountability, integrity, and public confidence in the administration and management of NPOs have been introduced through the DDA and PGR acts. In particular, information on the organisation and the purpose should be included in the foundation and establishment statutes, articles of association. Foundations and establishments are obliged to appoint a qualified member of the governing body, who is subject to DDA (Art. 3(1)(k) DDA). The latter should obtain sufficient information on the

NPO's relationships, in relation to their BOs specifically for purposes of monitoring the business relationship (including the transactions performed) (Art. 5(1), 7, 7a, 8 and 9 DDA; Art. 20 (1) DDO). According to PGR Art. 1059 NPOs are obliged to keep proper accounts, must retain account books, accounting vouchers, and business correspondence for a period of ten years. Nonetheless, the associations are only obliged to be entered in the commercial register (i) if they conduct business in a commercial manner for its purpose, or (ii) are subject to audit (PGR Art. 247(2)). Otherwise, the registration is voluntary. Moreover, no qualified member subject to the DDA is appointed in these associations.

(b) A number of trainings were conducted by the Office of Justice and the FIU aiming at raising and deepening the awareness of any persons engaging in the NPO sector in relation to TF risks. In addition, STIFA has published a factsheet for NPOs on TF risks, based on the findings of the NPO Risk Report (updated in November 2020). This factsheet was prepared jointly with FMA, FIU and the Fiscal Authority. VLGST as the central organisation to promote the interests of common-benefit organisations in Liechtenstein informs its members on a regular basis on various developments in the NPO sector. No outreach or educational programmes have been delivered for the donor community in relation to potential vulnerabilities of NPOs to TF abuse and risks.

(c) STIFA, FIU and FMA are regularly present at various events and training seminars, in which AML/CFT issues are discussed with representatives of the financial sector and NPOs. The authorities provided information that for the supervisory programme for the years 2020 and 2021, the bilateral supervisory meetings, which are conducted by STIFA with representatives of the high-risk NPOs, are held in order to raise their awareness with regard to TF and to show best practices. The Presentation was prepared and presented by the STIFA. The findings from the interviews carried out with representatives of common-benefit foundations, establishments and members of the VLGST in the course of elaborating the NPO Risk Report were used to update the existing factsheet of STIFA, which, together with the NPO Risk Report will be taken into account in upcoming seminars and trainings intended for the NPO sector. While no separate guidance has been developed, the factsheet is also addressed to associations that fall under the FATF definition of NPOs.

(d) Liechtenstein NPOs have been encouraged to conduct transactions via regulated financial channels during regular trainings held by STIFA and FIU and by the factsheet published by STIFA and FIU addressed to NPOs in relation to TF risks.

Criterion 8.3 –

Foundations and establishments- These group of NPOs are subject to AML/CFT and general administrative supervision. The AML/CFT supervision is conducted by the FMA in relation to the qualified members of the governing body in accordance with the DDA Act. At that, every business relationship and accordingly, every NPO has to be assigned to a risk category and risk-adequate measures pursuant to DDA/DDO have to be applied (see R.26).

The general (not AML/CTF specific) monitoring by authorities is carried out by the STIFA and the Commercial Register Division. The STIFA ensures that administration and use of assets by common-benefit foundations and establishments are in accordance with their statutory purpose. All common-benefit foundations and establishments must, without exception, be registered with the commercial register (Art. 537(1) PGR, Art. 552 § 14 (4) PGR). In addition, common-benefit foundations, establishments and associations are subject to fiscal monitoring. The ones that exclusively and irrevocably pursue common-benefit purposes without the intent of making a profit may apply to the Fiscal Authority to obtain tax exemption (Art. 4(2) Tax Act, Art. 3(1) and (2) Tax Ordinance). The Commercial Register Division, STIFA and the Fiscal Authority are obliged

to submit a SAR/STR to the FIU in case of ML/TF suspicion. Common-benefit foundations and establishments are subject to the supervision of STIFA, the focus of which is the compliance with the requirements set out in foundation law. Based on the outcomes of the NPO Risk Report the authorities have developed a supervisory programme for the years 2020 and 2021 in order to subject high-risk NPOs to additional supervisory measures and to enhance the awareness of any persons involved in the NPO sector with regard to TF risks (particular attention is given to high-risk NPOs). This is mainly done through bilateral supervisory meetings with high-risk NPOs (including high-risk associations).

Associations- These NPOs are not subject to AML/CFT or general supervision (apart from fiscal supervision), as no qualified members of the governing body are to be assigned, neither there is an obligation to register (i) if they do not conduct business in a commercial manner for its purpose, or (ii) are not subject to audit (Art. 247(2) PGR). Tax related supervision is exercised by the Fiscal Authority. Since 8 associations were classified as high-risk NPOs in the NPO Risk Report, bilateral supervisory meetings were also conducted with representatives of these high-risk associations. This however does not yet constitute a risk-based monitoring/supervision.

Criterion 8.4 –

(a) As provided under C.8.3 NPOs are supervised/ monitored directly by three authorities. STIFA is responsible to ensure that the assets of foundations and establishments under its supervision are managed and used in accordance with their purpose. FMA supervises persons subject to Art. 3 (1) a) to l) and n) to t) DDA. The Fiscal Authority is the competent body to ensure that those common-benefit foundations, establishments and associations comply with their filing obligations and fulfil the requirements on an on-going basis. Associations are not subject to direct supervision by FMA and STIFA. The authorities however have introduced the bilateral supervisory meetings mechanism based on the level of the risk of TF abuse for the NPOs.

(b) In the framework of AML/CFT supervision the FMA is entitled to apply a range of sanctions in relation to breaches of obligations stipulated under the DDA by the qualified members. This sanctioning regime is not directly imposed on the common-benefit structure but on the person subject to the DDA administering the common-benefit structure. The CC and CPC apply to the qualified members of the governing body appointed on the basis of Art. 180a(1) PGR as well as all other persons acting on behalf of NPOs.

In relation to administrative supervision, STIFA may apply to the Court of Justice to take the required orders, such as the dismissal primarily of members of the governing body or the revocation of resolutions taken by members of the governing bodies (Art. 552 § 29 (3) PGR).

In case of issues in relation to registered information, the Commercial Register Division shall call upon the party obliged to apply for the necessary amendment or removal within 14 days (Art. 968 (1) PGR). This request includes the threat of an administrative fine in the case of non-compliance. This applies to all legal entities registered with the Commercial Register, including associations. Sanctions may be applied by the Fiscal Authority in relation to the NPOs that do not fulfil their filing obligations on an on-going basis. Dissolution and liquidation of a legal entity is foreseen if it harms Liechtenstein's national interests or is detrimental to the country's reputation and disrupts its relationship with other states or international organisations (Art. 971 (1) (4) PGR) exercised by the Commercial Register Division.

Criterion 8.5 –

(a) The DDA (Art. 36) and the FIU Act (Art. 6) provide for the cooperation mechanisms among domestic authorities entrusted with AML/CFT matters. The legal basis ensures effective cooperation, coordination and information sharing regarding NPOs between the competent

authorities. Exchange of information among all competent authorities takes place in the framework of the PROTEGE WG. As STIFA is a division of the Office of Justice, STIFA is consequently also a member of the working group. In this context information sharing is particularly relevant between FMA and the FIU.

(b) The employees of the law enforcement authorities (Court of Justice, OPP and National Police (in accordance with Art. 20 to 22 CPC)) examine ML/TF cases. The competent authorities have appropriate investigative tools and powers to detect/examine NPOs possibly involved in TF. They take part in ML/TF trainings and seminars on an on-going basis. The OPP is ultimately responsible for an investigation and the prosecution of TF offences. There haven't been any specific NPOs related trainings, however the FIU, FMA and other competent authorities take part in ML/TF trainings and seminars on an on-going basis.

(c) In the framework of AML/CFT obligations persons subject to Art. 3 DDA are required to keep a record of compliance with the CDD duties and the reporting obligations for at least 10 years. The FIU, the Court of Justice and the OPP are empowered to require information for analytical and investigative purposes from persons subject to the DDA (Art. 19a (1) DDA, Art. 5a (1) and (b) FIU Act, Art. 92, 96 and 96b CPC).

The STIFA is entitled to demand information from supervised foundations/establishments and to inspect the books and documents (Art. 551 (2) in conjunction with Art. 552 §§ 26 and 29 PGR (establishments), Art. 552 §§ 26 and 29 PGR (foundations)). Common-benefit foundations and establishments must maintain appropriate records of the financial circumstances, all documents evidencing the course of business and movement of the administrated assets have to be maintained. Furthermore, a list of assets showing the asset position and asset investments must be kept (Art. 552 § 26 PGR, Art. 1045 (3) in conjunction with Art. 1059 PGR).

Associations are required to keep accounts on their income and expenditure as well as their financial situation by taking into account the principles of accounting. They are obliged to maintain records and keep documentary evidence in order to trace the course of business and development of assets (Art. 251a in conjunction with Art. 1045 (3) and Art. 1059 PGR). All records have to be kept for at least ten years. No other obligations exist in relation to associations. Nonetheless, the Court of Justice and the OPP can obtain information from any person (Art. 96 CPC).

(d) Whenever a STR/SAR has been submitted due to a suspicious transaction having indications of TF, the FIU analyses the information received in order to determine if the suspicion for ML/TF can be confirmed or not. In the event of a reasonable suspicion of ML/TF, FIU submits a report with the results of its analysis and any other additional information to the OPP (Art. 4 FIU Act). According to FIU Act, Art. 6(1) the FIU may exchange financial, administrative and law enforcement information and relevant documents required for the prevention of the TF with other domestic authorities, in particular the courts, the OPP, the National Police, the Office of Justice, the Tax Authority and the FMA. This also related to the cases of TF suspicion involving an NPO.

Criterion 8.6 – International requests for information regarding particular NPOs suspected of TF abuse are dealt with in the same way as any other international request for information. Liechtenstein has identified three point of contact: (a) the FIU is responsible for requests coming from its foreign counterparts (Art. 7 (1) and (2) FIU Act); (b) the FMA is point of contract for foreign supervisory authorities (Art. 37 DDA, Art. 26b FMA Act); and (c) the Court of Justice collects and handles requests for MLA of foreign law enforcement agencies (in cooperation with the Office of Justice). Mutual legal assistance in criminal matters is granted according to Art. 50

(1) MLA Act at the request by a foreign authority. Legal assistance within the meaning of this provision is every kind of support granted for foreign proceedings in criminal matters.

Weighting and Conclusion

Liechtenstein authorities have conducted an NPO sector risk assessment and identified the scope of high risk NPOs falling under the FATF definition. A number of regulatory measures are in place to ensure the transparency and accountability of NPOs, with some exceptions in relation to associations. Supervision/ monitoring is exercised by several authorities. Risk-based supervision is conducted by the FMA in relation to the qualified members of foundations and establishments (AML/CFT supervision), while the STIFA has been engaging in bilateral supervisory meetings (which is rather an awareness raising initiative) with high-risk NPOs. No risk-based monitoring/supervision, apart from fiscal supervision is in place in relation to associations.

R.8 is rated LC.

Recommendation 9 – Financial institution secrecy laws

In the 4th round MER of 2014, Liechtenstein was rated PC on R.4. The MER identified a number of deficiencies including: (i) the secrecy conditions under the FIU Act and the restrictions on the FMA's power to access and share confidential information domestically which could limit the FIU's ability to properly undertake its functions; (ii) it remained unclear whether the secrecy provisions in sector specific laws inhibited FIs' ability to share confidential information; and (iii) the requirement that foreign supervisors must be subject to the same secrecy provisions as contained in Art. 23 of the COPE for the FMA to exchange confidential information was considered too restrictive.

Criterion 9.1 - Professional confidentiality and exceptions thereto are provided for in: Art. 19a (1) and 28(4) of the DDA, Art. 96b of the CPC. While sectorial legislation provides for the professional secrecy provisions, obligations stipulated under the DDA take precedence over all these obligations.

(a) Access to information by competent authorities – FIs are required to provide all information to supervisory authorities on request and communicate all records and copies thereof to the supervisory authorities that they require to perform their oversight functions (DDA, Art. 28 (4)).

This obligation explicitly takes precedence over all obligations of confidentiality recognised by the government.

Similarly, a disclosure request by the FIU shall take precedence over all obligations of confidentiality state recognised (Art. 19a (1) DDA).

The phrase "obligations of confidentiality recognised by the government" refers to all secrecy provisions in the sectoral legislation (as indicated in the explanatory notes in the DDA bill) but has not, so far, been tested or confirmed by the courts.

Public prosecutors, as well as the National Police (based on a report sent to the OPP (see R.40)) can access information by way of a court order pursuant to Art. 96b CPC.

(b) Sharing of information between competent authorities – Sharing of information between domestic authorities is provided by the provisions of the DDA. In particular, Art. 36 (1) DDA states that "the Liechtenstein authorities are required to work together in close cooperation and to provide each on an unprompted basis or on request with all information required to fight ML, associated predicate offences, organised crime and financing of terrorism and to furnish information and pass on personal data, including personal data concerning criminal convictions and offences, and documents.

In relation to sharing with foreign counterparts, Art. 37 (2) (b) DDA was amended (1 April 2021) to make clear that a request for cooperation cannot be refused on the grounds of laws that impose secrecy or confidentiality requirements on FIs. Information sharing by the FIU and law enforcement with their overseas counterparts, is provided under R.40 analysis.

(c) Sharing of information between FIs – Sharing of information takes precedence over all officially recognised obligations of confidentiality in specified circumstances (DDA, Art. 16a). Namely: (i) in the context of a delegation under Art. 14 DDA (broadly equivalent to reliance as set out in R.17; and (ii) correspondent banking services as referred to in Art. 2 (1) (m) DDA (broadly equivalent to R.13 "correspondent banking").

In relation to wire transfers, information sharing is governed by the provisions of Regulation (EU) 2015/847, which applies directly in Liechtenstein. While these provisions require the sharing of specific payer information, the specific reference to taking "precedence over all officially recognised obligations of confidentiality" is not present in relation to wire transfers. At the same time, Art. 14 and 16 of the DDA also cover the operations, which are governed by the Payment Services Act (including the wire transfers) based on the scope of application of the DDA, thus the "precedence over all officially recognised obligations of confidentiality" in relation to wire transfers is indirectly covered by the DDA.

Weighting and Conclusion

R.9 is rated C.

Recommendation 10 – Customer due diligence

In the 4th round MER of 2014, Liechtenstein was rated PC on R.5. A number of deficiencies were identified including: (i) a blanket exemption from CDD that was not permissible under the FATF Recommendations; (ii) verification of the BO and customer that was a legal person were not always based on reliable sources; (iii) no obligation to carry out reviews of existing records as part of the ongoing CDD; (iv) high threshold for identification of existing anonymous or bearer passbooks, accounts, or custody accounts; (v) broad provisions that allowed not only for verification, but also for identification measures, to be delayed in certain circumstances; and (vi) CDD obligation for occasional transactions only extended to cash transactions.

As reported under c.1.6, the following activities - which are covered by the FATF definition of FI - are not subject to the DDA: (i) lending (own funds only); (ii) financial leasing; and (iii) issuing and managing paper-based means of payment.

AML/CFT requirements in Liechtenstein are not applied to business conducted remotely in Liechtenstein by EEA FIs or Swiss insurance undertaking and intermediaries operating with the scope of freedom to provide services.

Criterion 10.1 - Covered FIs are prohibited to hold accounts payable to bearer (including savings books and custodial accounts) and they may not hold either anonymous accounts (including safe deposit boxes, saving books and custody accounts) or accounts (including safe deposit boxes, saving books and custody accounts) in fictitious names (DDA, Art. 13 (3) (4)).

Criterion 10.2 – (a) Covered FIs are required to conduct CDD when establishing a business relationship (DDA. Art. 5(2)(a)); (b) Covered FIs are required to conduct CDD when carrying out occasional transactions amounting, in a single operation or in several apparently linked operations, to CHF 15 000 or more (DDA. Art. 5(2)(b) (1)); (c) Covered FIs are required to undertake CDD when carrying occasional transactions, when it constitutes a transfer of funds as defined by EU Regulation 2015/847 of more than CHF 1 000 (DDA. Art. 5(2)(b)(2)); (d) Covered

FIs are required to undertake CDD when there is suspicion of ML, a predicate offence of ML, organised crime, or TF, regardless of any derogation, exemption, or threshold (DDA. Art. 5(2) (d)); and (e) Covered FIs are required to undertake CDD when there are doubts about the authenticity or adequacy of previously obtained data on the identity of the contracting party or the BO (DDA. Art. 5(2)(c)), including the authenticity of any person purporting to act on behalf of the customer.

Criterion 10.3 - Covered FIs are required to identify the contracting party and verify the contracting party's identity by means of documents with "probative value" (DDA. Art. 5(1)(a) and Art. 6(1)). The term "contracting party" in the DDA covers both natural and legal persons (FMA Instruction 2018/7, point 2) acting on their own behalf or on behalf of a legal arrangement. The requirement applies to both business relationships and occasional transactions. Documents with "probative value" are defined in Art. 7 DDO (for natural persons) and in Art. 8 DDO (for legal persons), which ensures that the verification of the customer is done based on reliable and independent sources.

Criterion 10.4 - Covered FIs are required to ascertain that each person purporting to act on behalf of the contracting party is authorised to do so. FIs have an obligation to establish the identity of these persons and verify such particulars by consulting a supporting document (original or certified copy) or by means of signature authentication (DDO. Art. 6(3)).

Criterion 10.5 **-** Covered FIs are required to identify and verify the identity of the BO of a contracting party (DDA, Art. 5(1)(b)). FIs have to verify the identity of the BO by means of risk-based and adequate measures (distinct from "reasonable measures" required under the FATF Recommendation), to satisfy themselves that the person in question is actually the BO (DDA, Art. 7(2)). In all cases, covered FIs must understand and document the ownership and control structure (FMA guideline on RBA (2013/1), Art. 5.2).

BO means a natural person on whose initiative, or in whose interest, a transaction or activity is carried out or a business relationship is ultimately constituted (DDA, Art. 2(1)(e)). In the case of legal entities, the BO is also the natural person in whose possession or under whose control the legal entity ultimately is situated.

As explained under c.10.18, there is no requirement to identify the BO or take reasonable measures to verify identity: (i) where units in investment funds (excluding those subject to the Investment Undertaking Act) are held on behalf of third parties by subscribing banks, fund trading platforms or central securities depositories in Liechtenstein or from jurisdictions with due diligence and record-keeping requirements and supervisory standards that meet the requirements of Directive (EU) 2015/849, where ML/TF risk is assessed as low and other conditions are met; and (ii) for particular types of client accounts operated by lawyers (DDO, Art. 22b(4) and (5)). From a presentational perspective, the AT considers that these provisions amount to an exemption from applying CDD measures, rather than simplification of measures (which implies doing something less rather than not at all). The basis for these exemptions is considered under c.1.6.

It should be mentioned that, in some cases defined under DDO Art. 3(1)(d) to (i), a person other than a natural person can be deemed as a BO of the contracting party, which is not in line with FATF Recommendations, as, according to the Recommendations, the BO shall always be a natural person. The AT considers that these provisions amount to an exemption from applying CDD measures, the basis for which is considered under c.1.6.

Criterion 10.6 - Covered FIs are required to establish a profile of the business relationship, including in particular information about the origin of the deposited assets and the purpose and intended nature of the business relationship (DDA. Art. (8)(1)).

Criterion 10.7 - (a) Covered FIs are required to monitor business relationships, including transactions performed in the course of a relevant business relationship, in a timely manner, at a level that is commensurate with the risks involved to make sure that they are consistent with the business profile (DDA. Art. 9(1)). The business profile shall contain the following details: (i) the contracting party and BO; (ii) the authorised agents and bodies authorised to act for the contracting party; (iii) origin of the assets deposited (source of funds) (SoF); and (iv) financial background of the total assets (source of wealth) (SoW), including occupation and business activity of the actual contributor of the assets; and (v) intended use of the assets (DDO, Art. 20). Monitoring of a business relationship – including transactions – must also be carried out in accordance with the risk profile of a customer (FMA-Instruction 2018/7, point 5.5). The level of information held shall be in accordance with the risk posed by a specific business relationship. In any case – irrespective of the risk, covered FIs must be able, on the basis of provided information, to identify any deviation or anomalies in relation to past experience with the client and the client's business relationship (RBA guideline, Art. 5.31).

(b) Covered FIs are required to ensure that the data and information in the business profile – based on documents with probative value (see c.10.3 and c.10.5) - is kept up to date, by running checks at intervals appropriate to the risk involved, to establish whether the information and data contained in the business profile is still current (DDA. Art. 8(2)). Changes relevant to the business profile must also be recorded to ensure that the profile remains relevant (FMA Instruction 2018/7, point 5.4.2).

Criterion 10.8 - Covered FIs are required in the case of a "legal entity" to apply both risk-based and adequate measures in order to determine and understand the ownership and control structure of the contracting party (DDA, Art. 7(2) and FMA Instruction 2018/7, point 5.3). However, the FATF Recommendations call not for measures to be applied, but rather for a FI to understand the nature of the customer's business and its ownership and control structure. The definition of "legal entity" covers a legal person, company, trust or "other collective or asset entity" (legal arrangements similar to trusts), irrespective of legal form (DDA, Art. 2(1)(f)). Covered FIs are required also to understand the purpose and the business of a customer that is a legal person (FMA Instruction 2018/7, point 5.4.1).

Criterion 10.9 - The following information must be obtained by covered FIs for customers that are legal entities: (i) name or corporate name; (ii) legal form; (iii) address of registered office (but not also principal place of business, where different); (iv) state of domicile; (v) date established; and (vi) place and date of entry in a commercial register (both domestic and foreign registers) (DDO, Art. 6(1)(b)). For legal entities not entered in a commercial register, the following documents need to be obtained: (i) an official certificate issued in Liechtenstein; (ii) statute, formation document or formation agreement; (iii) certification of the information specified under DDO Art. 6(1)(b) by the appointed auditor of annual accounts; (iv) official licence to conduct activities; or (iv) written extract from a trustworthy privately maintained directory or equivalent database (DDO, Art. 8(2)). For legal entities, covered FIs must obtain and record the names of the bodies or trustees acting formally on behalf of the legal entity in the relationship with the person subject to the DDA (DDO, Art. 6(1)(b)). This requirement refers not to all persons having a senior management position in the legal entity, but only to those authorised to act on its behalf.

Covered FIs are required to obtain either an extract of the company register (for entities in a commercial register) or the statute, formation document or formation agreement (for entities not

registered in a commercial register). The authorities have explained that such sources would encompass information on powers that regulate and bind the legal entity as well as the names of the relevant persons having a senior management position in the legal entity but have not provided legal sources to support this.

***Criterion* 10.10**[41] - C.10.5 explains the requirement to identify and take risk-based and adequate measures (distinct from "reasonable measures" required under the FATF Recommendations) to verify the identity of the BO of a contracting party. The following shall be deemed to be the BO of a corporate body[42] or company without legal personality[43]: (i) natural persons who ultimately directly or indirectly hold or control a share or voting right amounting to 25% or more or have a share of 25% or more in the profit; (ii) natural persons who ultimately directly or indirectly exercise control over management in another way; or (iii) if, after having exhausted all possible means, natural persons who are members of the executive body if no person can be identified under (i) or (ii) (DDO, Art. 3(1)(a) no. (1) and (2)). All subsequent stages are used if it is not possible to identify the BO by using the previous stages.

Criterion 10.11 - C.10.5 explains the requirement to identify and risk-based and adequate measures (distinct from "reasonable measures" required under the FATF Recommendations) verify the identity of the BO of a contracting party. The following shall be deemed to be the BO of a foundation, trusteeship and establishment with a structure similar to that of a foundation or trust enterprise: (i) natural persons, who are effective, non-fiduciary sponsors, founders or settlors, irrespective of whether they exercise control post establishment; (ii) natural or legal persons who are members of the foundation board, board of directors of an establishment (with a similar structure to an establishment) or of the trustee; (iii) any natural persons who are protectors or persons in similar or equivalent functions; (iv) natural persons who are beneficiaries; (v) if the beneficiaries have yet to be determined, the group of persons in whose interests the legal entity is primarily established or operated; and (vi) the natural persons who ultimately control the legal entity through direct or indirect ownership rights or in any other way (DDO, Art. 3(1)(b)). It should be mentioned that, in the case of a member of the board or a foundation or trustee, a legal person can be deemed as a BO of the contracting party which is not in line with the FATF Recommendations (DDO, Art. 3(1)(b)(2)).

In the case of (v), covered FIs shall obtain sufficient information concerning the persons in whose interest the legal entity has been established or is primarily operated, in order to ensure that they are able to establish their identity at the time of paying out (DDA, Art. 7a(1)). FIs will collect information regarding potential beneficiaries by inspecting statutes, "letters of wishes" and by-laws (FMA Instruction 2018/7). The identity of the recipient (who will at that time become a beneficiary) must be established and verified by covered FIs at the time of paying out, except by banks that have a relationship with the legal entity, where this obligation applies only to distributions from assets that are entered in their books (DDA. Art. 7a (2)). Whilst this ensures

---

[41] Foundations are regarded as the civil law equivalent to a common law trust, as they may be used for similar purposes. Accordingly, they are assessed under c.10.11 (legal arrangements). This approach ensures that the settlor and beneficiaries etc of a foundation are identified and verified as a BO.

[42] Defined as: (i) associations; (ii) public limited companies; (iii) partnerships limited by shares; (iv) companies limited by units; (v) limited liability companies; (vi) cooperative societies; and (vii) mutual insurance associations and auxiliary funds (Persons and Companies Act, Title 4).

[43] Defined as: (i) joint provisions; (ii) unregistered partnerships; (iii) general partnerships (open partnerships); (iv) limited partnership; (v) consortia; (vi) silent partnerships; and (vii) community of property (Persons and Companies Act, Part 3).

that all discretionary beneficiaries who are to benefit from funds held by the bank will be identified and verified at the time of pay out, banks may not be required to take reasonable measures to verify the identity of all of the beneficiaries for a particular trust in line with c.10.11(a). This limitation is considered to be minor since the authorities explained that trust assets tend to be held at one bank only. If the recipient of the distribution is a legal entity, its BO shall be identified and verified (DDA, Art. 7a(1) and (2)).

Covered FIs, in the process of conducting the above-mentioned measures, may rely on a domestic TCSP to immediately convey the information that a distribution is about to be made and without being requested to do so - where assets that are held in the books of the other FI are to be distributed (but not otherwise) (DDA, Art. 7a (3) and (4) as modified by FMA Instruction 2018/7).

Criterion 10.12 - For life assurance policies and other insurance taken out for investment purposes, insurance undertakings shall perform the following duties: (i) for beneficiaries who are identified as specifically named natural persons or legal entities, they shall record the name of that person; and (ii) for beneficiaries whose identity is established from characteristics or by category or in another way, they shall obtain sufficient information in respect of these beneficiaries in order to make sure that they are able to establish their identity at the time of paying out. For both cases, insurance undertakings shall establish the identity of the beneficiary of life assurance policies and other insurance with an investment related objective at the time of paying out and take appropriate steps to verify that identity. (DDA, Art. 7b (1) and (2)). The requirements of Art. 7b apply only to insurance undertakings and not generally to all FIs as is required under FATF Recommendations.

Criterion 10.13 - FIs are required to conduct a risk assessment for each business relationship. In conducting this customer risk assessment, they have to take into account customer-related risks, including risks in relation to the contracting party, the BO, the beneficiaries of legal arrangements as well as the beneficiaries of insurance policies (DDA, Art. 9a and Annex 2, section A). It should be mentioned, however, that Annex 2 section A refers only to examples when beneficiaries of insurance policies are resident in higher risk geographical areas or have been a politically exposed person and does not consider such risk factors that are connected with the reputation of the person, or his/her commercial or professional activities. Consequently, the risks associated with the beneficiary are not completely covered. If higher risks are identified in relation to the beneficiary, EDD has to be applied (DDA, Art. 11(1)). Where the beneficiary is a legal entity, the identity of its BO must be established and verified in all cases, and not just those where a higher risk is identified (DDA, Art. 7b(2)).

Criterion 10.14 - All information and documents required for the identification and verification of the identity of the contracting party and the BO must be complete and available in an appropriate form when the business relationship commences, or when an occasional transaction is carried out (DDO, Art. 18 (1)). There are two exceptions to this rule. First, a covered FIs may complete CDD measures for verifying the identity of a new customer or BO after establishment of a business relationship provided that: (i) it is necessary to maintain the normal conduct of business; and (ii) ML/TF risks are low. In such situations, verification must be completed as soon as possible after the first contact and covered FI must ensure that no outward movement of assets takes place in the meantime (DDO, Art. 18(2)). Whilst there is no explicit reference to a requirement to manage risk, this may be inferred from the requirement for risks to be low. Second, banks and investment firms may proceed with the opening of a bank account – including accounts through which securities transactions may be conducted – provided that adequate safeguards are put in place to ensure that transactions (including inward and outward payments) are not conducted until the duties of CDD have been performed in full. Whilst there is no reference

to the conditions listed under this criterion, the substance of this arrangement is that the account cannot be used until verification has been completed (DDO, Art. 18(3)).

Criterion 10.15 - There is no explicit requirement under the first exception that covered FIs should adopt risk management procedures concerning the conditions under which a customer may utilize the business relationship prior to verification. However, FIs are required to ensure that no outward movement of assets take place until the verification has been carried out (DDO, Art. 18(2)). Under the second exception, it is not possible to use the relationship prior to verification.

Criterion 10.16 - Revised full CDD measures introduced by the Law of 4 May 2017 amending the DDA had to be applied to all existing customers according to transitional provisions of the DDA as from 1 June 2018. For business relationships commenced prior to 1 January 2016 to which enhanced measures were applicable, there was a requirement for the identification and verification of the identity of the BO to be repeated by no later than 31 December 2018. The requirement for other relationships established prior to 1 January 2016 was for verification of the identity of the BO to be repeated by no later than 31 December 2020. Within this second category (relationships to which enhanced measures do not apply), there were no provisions requiring covered FIs to apply CDD on the basis of materiality and risk, or, when determining appropriate times, to take into account whether and when CDD measures had previously been undertaken and the adequacy of the data obtained. For the sake of completeness, other measures related to the revision of the FATF Recommendations (that took place prior to January 2016) had to be applied immediately to all existing customers.

However, it does not appear that the above transitional arrangements apply in respect of some business relationships established prior to 1 January 2001 where BO information is not held (DDA, Art. 35). The authorities have explained that only 122 accounts are affected, with an average balance of CHF 95 000. In such cases, no outflow of assets shall be permitted as long as the requisite information and records are not available. The outflow of assets shall be permissible if all the following conditions are met at the same time: (i) assets do not exceed CHF 25 000; (ii) there is no suspicion on ML/FT; (iii) operation of the transfer is traceable and the FI knows the recipient; and (iv) business relationship is terminated immediately after the transfer. Whilst these requirements take account of risk and materiality, no deadline has been set for relationships to be remediated, and it is not clear that an open-ended arrangement can be considered to meet the requirement to apply CDD to existing relationships "at appropriate times". Given the materiality of the relationships involved, the shortcoming is considered to be minor.

Criterion 10.17 - Covered FIs must establish criteria to identify business relationships and transactions involving higher risk and categorise business relationships/transactions accordingly (DDA, Art. 9a(4)). Covered FIs are required to perform EDD – examples are set out in Annex 2 Section B of the DDA – to business relationships presenting higher AML/CFT risks (in addition to the regular due diligence obligations) in order to address or reduce the increased risk (DDA, Art. (11)(1)). PEP and correspondent relationships are to be assumed as presenting a higher risk in all cases (DDA, Art. 11(4) and (5)). Covered FIs shall also conduct enhanced monitoring of the following business relationships and transactions and, to the extent possible, investigate their background/purpose and record the results in writing: (i) complex structures or transactions; (ii) unusually large transactions; (iii) unusual transaction patterns; and (iv) transactions that have no apparent financial purpose or discernible lawful purposes (DDA, Art. (11)(6)). With regard to business relationships or transactions involving states with strategic deficiencies, covered FIs shall apply EDD as set out in Annex 2 of Section B of the DDA (DDA, Art. 11a(1)) and such other matters as may be prescribed by the Government.

Criterion 10.18 - Covered FIs have an obligation to conduct a business risk assessment during which they shall pay special attention to listed factors for possible indicators of lower risk and the NRA (DDA, Art. 9a (1) (2) (3) and Annex 1). The application of SDD to business relationships or transactions is only permissible, if, after conducting such a risk assessment, covered FIs deem that there is only a low risk (rather than lower risk – as required under the FATF Recommendations) with reference to ML, organised crime and TF (DDA, Art. (10)(1) and (2)). In addition, it is specified that SDD may be applied only if persons subject to the DDA have identified a low risk and have ensured that the business relationship or transaction is indeed associated with a low risk (RBA guideline of the FMA, Art. 5.5). Examples of simplified measures are provided (DDA, Annex 1, Part B), but it is not specified that selected measures must be commensurate with risk.

In addition, the DDO lists two particular cases where SDD may be applied: (i) where units in investment funds (excluding those subject to the Investment Undertaking Act) are held on behalf of third parties by subscribing banks, fund trading platforms or central securities depositories in Liechtenstein or from jurisdictions with due diligence and record-keeping requirements and supervisory standards that meet the requirements of Directive (EU) 2015/849, where ML/TF risk is assessed as low and other conditions are met; and (ii) to particular types of client accounts operated by lawyers (DDO, Art. 22b (4) and (5)). However, since the effect of the provisions is to exempt a covered FI from identifying and verifying the identity of the BO, this is considered instead under c.10.5.

Application of SDD under Art. 10 of the DDA is excluded if there is a suspicion of ML, a predicate offence to ML, organised crime, or TF or if there are factors and possible indications of a potentially higher risk (DDO, Art. 22b(6)).

Criterion 10.19 - (a) - Covered FIs are not allowed to establish a business relationship or carry out an occasional transaction if the due diligence duties cannot be performed (DDA, Art. 5(3)(a)). An existing business relationship must be discontinued if due diligence duties cannot be performed, irrespective of other statutory or contractual provisions (DDA, Art. 5(3)(b)). Moreover, if, during repetition of the identification and verification process, any doubts persist with regard to the data obtained on the contracting party and BO, covered FIs must terminate the business relationship (DDO, Art. 15(1)).

However, termination of a business relationship is not required in a case where it was opened before 1 January 2001 and BO information is not held (see c.10.16), where current CDD measures do not apply. Despite the measures underlined in the Art. 35 of the DDA, this approach is not in line with c.10.19.

(b) In cases listed under (a), covered FIs are required to verify whether an SAR/STR should be sent or not (DDA, Art. (5)(3)(a) and (b)).

Criterion 10.20 - In cases where covered FIs form suspicion of ML/TF and reasonably believe that performing CDD measures will "tip-off" the customer, they shall not pursue the CDD process and must instead immediately submit a report to the FIU (DDO, Art. 26a).

Weighting and Conclusion

The key elements of CDD are in place in Liechtenstein, except that covered FIs are not always required to identify the BO of a customer under exemptions set out in the DDA – which are not

based on risk (considered under c.10.5 and c.1.6). The majority of these exemptions, however, are commonly found elsewhere.
Whilst exemptions from the scope of application of the DDA (see c.1.6) are relevant here, they are considered only minor in light of the country's focus on wealth management.

R.10 is rated LC.

Recommendation 11 – Record-keeping

In the 4th round MER of 2014, Liechtenstein was rated LC on R.10. There was no express obligation to keep business correspondence and no measures in place to ensure that transaction records permitted the reconstruction of individual transactions in all cases.

The introduction to R.10 lists activities to which the DDA does not apply.

Criterion 11.1 - Covered FIs shall keep a record of compliance with duties of due diligence and for this purpose they shall establish and maintain due diligence files (DDA, Art. (20)(1)). The due diligence files shall contain records with details of transactions (DDO, Art. 27(1)(d)). Transaction-related documents, business correspondence and vouchers shall be retained for ten years from conclusion of the transaction or from the date the document was prepared (which will not differ significantly from the transaction date) (DDA, Art. 20(1)). The requirement concerns both domestic and international cases, as no distinction is made between these two. The information to be transmitted for wire transfers - as referred to in Art. 23(d)(1) DDO - must also be recorded in the due diligence file and must be kept for 10 years (DDO, Art. 27(1)).

Criterion 11.2 - Covered FIs have an obligation to establish and maintain due diligence files that contain records and vouchers "issued and consulted" in order to comply with the DDA and DDO. Client-related documents, business correspondence and vouchers are to be retained for ten years from the end of the business relationship or after the execution of an occasional transaction (DDA, Art. 20(1)). The term "client-related" is defined to include, amongst other things: (i) the documents and records that have been used to identify and verify the contracting party and the BO (and other records obtained through CDD measures); (ii) information about business profile (which addresses c.10.6); and (iii) documents, records and vouchers concerning any investigation conducted to monitor a business relationship (DDO, Art. 27(2)). Whilst there is no explicit requirement to keep the results of any analysis undertaken as part of CDD measures, it is considered that these are covered by the generality of the record-keeping requirements.

Criterion 11.3 - The origin and execution of business transactions must be traceable and entries in business records and other required records must be complete, correct, timely, and orderly (DDA, Art. 2(1)(q) in combination with DDA, Art. 20(1) and DDO, Art. 27(2) in combination with DDO, Art. 27(1)(d-e) and (h)). The effect of this requirement is to make it possible to reconstruct individual transactions, including the amount and currency, though this is not explicitly stated.

Criterion 11.4 - Due diligence files shall be set up and stored in such a way that requests from competent domestic authorities and courts, auditors, and supervisory bodies can be met in full within a reasonable timescale - interpreted by the authorities to mean time that is necessary in a properly run business operation to compile the relevant documents (DDO, Art. 28(1)(c)). This requirement is not entirely consistent with the Standard, which calls for records to be available "swiftly". A "reasonable timescale" cannot always guarantee that files will be available "swiftly", as the understanding of what is meant by the term may differ between the private and public sector.

Weighting and Conclusion

The provisions of the DDA, together with the DDO, largely cover record-keeping requirements. Still, there remain some minor deficiencies, e.g., it is not ensured that due diligence files are available "swiftly". Shortcomings underlined under the conclusion to R.10 with regard to the scope of application of the DDA are also relevant here.

R.11 is rated LC.

Recommendation 12 – Politically exposed persons

In the 4th round MER of 2014, Liechtenstein was rated LC on R.6.

The introduction to R.10 lists activities to which the DDA does not apply.

Criterion 12.1 - A politically exposed person means a natural person who is, or was, up to one year earlier, entrusted with a prominent public function and their immediate family members, or persons known to be close associates of a such person (DDA, Art. 2(1)(h)). The following offices shall be deemed to be prominent public functions within the meaning of Art. 2(1)(h) of the DDA, unless they are only junior or middle-ranking offices: (i) heads of state, heads of government, ministers, deputy ministers, secretaries of state and prominent party officials; (ii) Members of Parliament or members of comparable state legislative bodies; (iii) members of supreme courts, constitutional courts or other high-ranking judicial bodies whose decisions are not subject to further appeal, except in exceptional circumstances; (iv) members of the courts of auditors or the managing board and executive bodies of central banks; (v) ambassadors, *chargés d'affaires* and high-ranking officers in the armed forces; (vi) members of the managing board, executive bodies or supervisory bodies of state-owned enterprises; and (vii) directors, deputy directors and members of the executive body, as well as similar office holders at international governmental organisations (DDO, Art. 2(1)).

In contrast to Art. 2(1)(h) of the DDA, the FATF Recommendations cover persons "who are or have been entrusted with public functions," and do not specify a time period during which an individual must remain defined as a PEP after relinquishing their prominent public function. FATF guidance points towards a more RBA and (specifically) not a prescribed time limit. This point is partially addressed through inclusion of a relationship with former PEPs as an indicator of a potentially higher risk which may be subject to application of EDD measures (DDA, Annex 2 section A(a)(10)). It is also explained that the risk arising from a PEP does not drop abruptly when their function comes to an end and that a careful examination of each individual case is necessary in order to be able to make a risk-appropriate decision. A decision to assign the business relationship to a lower risk category should be justified and documented (FMA Guideline 2013/1, point 5.8.2). However, under the DDA, risk-based measures are not required to be applied to former PEPs that continue to present a standard or lower PEP risk – where PEP risk has not yet been fully extinguished. This is not in line with R.12 and affects the overall rating.

a) Covered FIs are required to employ adequate, risk-based procedures to determine whether the contracting party, the BO, or the recipient of discretionary distributions from a trust is a covered PEP (DDA, Art. 11(4)(a)). Moreover, FIs, as far as it is possible, have to use IT-based systems to identify PEPs (DDA, Art. 9b).

b) Covered FIs are required to obtain the approval of at least one member of general management (at a senior level) before establishing or continuing a business relationship related to a covered PEP (DDA, Art. 11(4)(b)). Approval of a member of the executive body on continuing of the business relationship is also required on an annual basis (DDA, Art. 11(4)(c)). This additional requirement, which goes beyond FATF Recommendations, does not cover persons holding important offices in Liechtenstein.

c) The requirement to take reasonable measures to establish the SoW and the SoF of a customer and the BO according to the responses of authorities, is covered by the general obligation on covered FIs to establish a profile of the business relationship, including in particular information concerning the "origin of the assets" (DDA, Art. 8(1) and DDO, Art. 20(1)(c) and (d)) – see c.10.7. The effect of this is that there is a requirement to establish the SoF and SoW for the customer and BO.

d) Covered FIs are required to conduct continuous and enhanced supervision of the business relationship with a PEP (DDA, Art. 11(4)(d)).

Criterion 12.2 – Save for one difference, the same provisions that apply to foreign PEPs also apply to domestic PEPs and persons entrusted with a prominent function by an international organisation. The difference is that covered FI may carry out a risk assessment of the business relationship in the case of persons holding important public offices in Liechtenstein and, if no higher risks have been identified, apply regular due diligence (DDO, Art. 23(2)).

Criterion 12.3 - PEP requirements apply also to immediate family members of PEPs and persons known to be close associates of PEPs (DDA, Art. 2(1)(h)). Family member is defined as being the spouse, partner considered equivalent to a spouse under national law, children and their spouses or partners, and parents and siblings (DDO, Art. 2(2)). A close associate is a natural person who: (i) is known to have joint BO of a legal entity together with a PEP or maintains other close business relations with a PEP; (ii) has sole BO of a legal entity which is known to have been set up for the de facto benefit of a PEP; or (iii) is connected socially or politically with a PEP (e.g., girlfriend/boyfriend and prominent members of the same politically party (DDO, Art. 2(3) and FMA instruction 2018/7, General Part, point 6 (Annex 6)). In line with the EU AMLD, the definition does not include a case when a person has joint BO of a legal entity that has been set up for the de facto benefit of a PEP.

Criterion 12.4 - In relation to life insurance policies, covered FIs are required to take appropriate measures to determine whether the beneficiary identified in accordance with Art. 7b (2) of the DDA (which includes the BO of a beneficiary that is a legal entity) is a PEP (DDA, Art. 11(4a)). These measures must be undertaken without failure prior to payment of the insurance proceeds (DDA, Art. 11(4a)). If a PEP is identified, the covered FI must: (i) inform at least one member of the executive body before the insurance proceeds can be paid out; and (ii) place the entire business relationship under continuous, enhanced supervision (DDA, Art. 11(4a)). If higher risks have been identified, a covered FI must also examine whether a report must be submitted to the FIU (FMA Guideline 2013/1, part 5.2.1).

Weighting and Conclusion.

There are only minor shortcomings. Risk-based measures are not required to be applied to former foreign PEPs that present a standard or lower risk, i.e., PEP risk has not been fully extinguished and the definition for close associates of PEPs is considered to be too narrow. Shortcomings underlined under the conclusion to R.10 with regard to the scope of application of the DDA are also relevant here.

R.12 is rated LC.

Recommendation 13 – Correspondent banking

In the 4th round MER of 2014, Liechtenstein was rated LC on R.7. Provisions on cross-border correspondent banking did not apply for respondent institutions in other EEA member states and

there was no requirement for Liechtenstein correspondent institutions to ensure that respondent institutions' AML/CFT controls were adequate and effective.

Criterion 13.1 – The definition of correspondent banking is in line with Directive (EU) 2015/849. It covers the provision of banking services by one bank (the correspondent) to another bank (the respondent) (DDA, Art. 2(1)(m)(1)). This includes the holding of a current account or other liability account and the provision of services associated therewith, such as cash management, international fund transfers, cheque clearing, services in connection with payable-through accounts and foreign exchange. It also includes relationships amongst other FIs, where similar services are provided by a correspondent institution to a respondent institution including relationships established for securities transactions or funds transfers (DDA, Art. 2(1)(m)(2)).

a) In cross-border correspondent banking relationships, covered FIs are required to have sufficient information about the respondent institution to: (i) understand the nature of its business; and (ii) be able to determine from publicly available information the reputation of the institution and the quality of its supervision (DDA, Art. 11(5)(a)). When obtaining information on the reputation of the respondent institution, this must involve determining whether the respondent institution has been investigated or been subject to supervisory measures for ML/TF (DDO, Art. 16(2)).

b) Covered FIs are required to assess the respondent institution's AML/CFT controls (DDA, Art. 11(5)(b)).

c) Covered FIs are required to obtain approval from at least one member of general management (at a senior level) before establishing new correspondent relationships (DDA, Art. 11(5) (c)).

d) Covered FIs are required to document the respective responsibilities with respect to fulfilment of due diligence requirements by the two institutions involved (DDA, Art. 11(5)(d)). In addition to documenting respective responsibilities, it must be ensured that the respective responsibilities under due diligence legislation are clearly understood (DDO, Art. 16(3)).

Criterion 13.2 - Covered FIs are able to establish or continue a correspondent relationship with a respondent that permits its account to be used directly by customers for transacting on their own behalf (payable through account).

a) Where "payable-through accounts" are permitted (transitory accounts), covered FIs that provide correspondent banking services for respondent institutions shall satisfy themselves that the respondent institution: (i) has verified the identity of persons having direct access to the accounts of the correspondent institution; and (ii) has subjected these persons to constant due diligence scrutiny (DDO, Art. 16(1)(a) and (b)).
b) Covered FIs should ensure that, during the correspondent relationship, the respondent institution would be able, at the request of the correspondent institution, to provide the data required to comply with due diligence regulations (DDO, Art. 16(1)(c)).

Criterion 13.3 - Covered FIs are prohibited from conducting correspondent banking relationships with shell banks (DDA, Art. 13(1)). They shall take appropriate measures to ensure that they do not conduct any business relationships with undertakings allowing shell banks to use their accounts, including custody accounts or safe deposit boxes (DDA, Art. 13(2)). Unlike the definition of shell bank in the glossary to the FATF Recommendations, there is a requirement in the DDA for the financial group to be "regulated" but not explicitly subject to effective consolidated supervision.

Weighting and Conclusion

There is only one minor shortcoming. **R.13 is rated LC.**

Recommendation 14 – Money or value transfer services

Liechtenstein was rated LC for former SR VI in the 3rd round MER, the report commenting that the threshold for obtaining customer identification was too high. SR VI was not assessed in the 4th round MER in 2014.

Consistent with measures summarised under c.14.2, the authorities have explained that there are no hawala operators in Liechtenstein.

Criterion 14.1 - Natural or legal persons that are MVTS operators must be licensed and regulated as banks or payment service providers (PSPs) in Liechtenstein (Banking Act, Art. 3(3)(e) applying Art. 2(2) of the Payment Services Act, and Payment Services Act, Art. 7(1)). No additional licence is required in Liechtenstein for EEA MVTS operators that operate through an establishment in Liechtenstein or which operate within the scope of freedom to provide services where licensed in the EEA by a responsible supervisory authority (home member state). In such a case, home competent authorities must notify the FMA in advance in the case of such operations – see c.26.2.

PSPs are defined to include e-money institutions and payment institutions when they undertake "payment services" – including money remittance business. Money remittance business is defined so as to capture the FATF concept of MVTS (Payment Services Act, Art. 4(1)(17)).

Criterion 14.2 - Providing MVTS without a licence constitutes an offence (Payment Services Act, Art. 109).

The FMA is authorised to demand information and materials from any person suspected of carrying out PSP activity without a licence (Payment Services Act, Art. 35(8)). In urgent cases, the FMA may order immediate cessation and termination without prior warning and without imposing a deadline. In addition, provision of payment services without a licence or registration can attract a penalty of imprisonment or a fine up to 360 "daily rates" (Payment Services Act, Art. 109(1)(b)). "Daily rates" are calculated by the courts based on the particular circumstances of the convicted person, with a minimum of CHF 10 and a maximum of CHF 1 000 (fine up to CHF 360 000). (See c.35.1).

The authorities have explained that the FMA regularly monitors media (including potential advertisements placed by such businesses and social media) "and other sources", e.g., the internet and general public, and has "regular information exchanges" with the private sector (whistleblowing of non-authorised business activities) and other public authorities in order to identify unauthorised MVTS activities. There have been no indications of unauthorised activities during the current review period.

Criterion 14.3 – MVTS operators are supervised for compliance with obligations by the FMA (DDA, Art. 23(1)(a)). This includes EEA PSPs that operate through an "establishment" in Liechtenstein, which covers branches, agents, and representative offices. It does not include EEA PSPs operating within the scope of freedom to provide services.

Criterion 14.4 - The FMA maintains a publicly available register of agents acting on behalf of Liechtenstein PSPs in: (i) Liechtenstein; or (ii) another EEA Member State (Payment Services Act, Art. 16(1)(c)). Upon entry in the register, the agent may commence providing payment services on behalf of the licensed PSP (Payment Services Act, Art. 25(2)). PSPs are not permitted to operate through agents (or branches) outside the EEA (Payment Services Act, Art. 25 and 27).

Criterion 14.5 - MVTS providers must include agents in their group-wide policies and procedures and must monitor the agents' compliance (DDO, Art. 25(3)).

Weighting and Conclusion

R.14 is rated C.

Recommendation 15 – New technologies

In the 4th round MER of 2014, Liechtenstein was rated LC on R.8 as there was no express obligation for FIs to have in place policies or measures to prevent use of technological developments for ML/FT, and no provisions in place requiring FIs to implement policies and procedures to address the risks associated with non-face-to-face transactions as part of ongoing due diligence.

Amended R.15 focusses on assessing risks related to the use of new technologies, in general, and imposes a comprehensive set of requirements in relation to VASPs. The FATF revised R.15 in October 2018 and its interpretative note in June 2019 to require countries to apply preventive and other measures to VAs and VASPs. In October 2019, the FATF agreed on the corresponding revision to its assessment Methodology and began assessing countries for compliance with these requirements immediately.

The introduction to R.10 lists activities to which the DDA does not apply.

The following trustworthy technology (TT) service providers are regulated and supervised under the Law on Tokens and TT Service Providers 2019 (TVTG) and DDA: (i) token[44] issuers – persons who publicly offer tokens in their own name or in the name of a client; (ii) TT key and token depositaries – who safeguard TT keys (private keys) and tokens for clients, e.g. in a safe or collective wallet, and who execute transactions for third parties; (iii) TT protectors - who hold tokens on a TT system in their own name or on account for a third party (as nominee); (iv) physical validators – who ensure the enforcement of rights in accordance with an agreement, in terms of property law, represented in tokens on TT systems; (v) TT exchange service providers – who exchange fiat currencies for tokens and vice versa, and tokens for tokens; and (vi) TT agents[45] – persons who distribute or provide one or more of the aforementioned TT services in Liechtenstein for foreign TT service providers (TVTG, Art. 2(k) and (m) to (q) and (u)). In addition, the following services are regulated and supervised under the DDA only: (i) token issuers who are not required to be registered under the TVTG who issue tokens on their own behalf or in a non-professional capacity on behalf of a client –under a prescribed threshold; and (ii) operators of trading platforms. With the exception of token issuers who are not required to be registered under the TVTG, these persons are referred to as TT Service Providers in the DDO.

Of the above TT Service Providers, the following are considered to be covered by the FATF definition of VASP: (i) TT key and token depositaries; (ii) TT protectors; (iii) TT exchange service providers; (iv) administering of VAs or instruments enabling control thereover, but only to the extent that tokens are held as a nominee; and (v) TT agents – to the extent that they perform an activity covered by the FATF definition of VASP. There is no general regulation of transfers of VAs nor overriding provision dealing with the provision of financial services related to an issuer's offer and/or sale of a VA (e.g., acting as market maker) which is called for by the FATF Recommendations. The authorities have explained that, instead of regulating these activities, they

---

[44] "Token" is defined in Art. 2 *(1) (c)* of the TVTG as "a piece of information on a trustworthy technology (TT) system which can represent claims or rights of membership against a person, rights to property or other absolute or relative rights; and is assigned to one or more TT Identifiers". Not all tokens are a VA, but all VAs are tokens.

[45] TT agents are subject to registration and supervision under the DDA to the same extent as other TT service providers. The only exception that is made is with respect to travel rule requirements. If the service provider abroad for which the TT agent is operating must comply with the requirements of the travel regulations abroad and, if it is ensured that this covers all relevant transfers of the TT agent, the TT agent is not subject to the travel rule requirements. In every other case TT agents are subject to the travel rule requirements in Liechtenstein.

regulate all persons that provide such a service (TT key or token depositary, TT protector or TT exchange service provider, and TT agents). Hereafter, (i) to (v) are referred to as "covered VASPs" and tokens referred to as VAs.

Criterion 15.1 - In the context of NRA II and NRA-VA (as updated), Liechtenstein has demonstrated a clear understanding of risks in relation to the development of new products and business practices and use of new or developing technologies.

With regard to covered FIs, they have an all-encompassing obligation to conduct ML/TF risk assessments in the context of DDA obligations. In this respect, the DDA requires covered FIs to ensure that the risks arising from the development of new products or commercial practices, or from the use of new or developing technologies are taken into account in the course of business level ML/TF risk assessments (business risk assessment) (DDA, Art. 9(2)). In this respect, covered FIs must pay special attention to the factors contained in both Annexes 1 and 2 of the DDA (respectively factors and indicators for the application of SDD and EDD). Annex 2 refers to new products and new business models, including new distribution mechanisms, and the use of new or developing technologies for both new and pre-existing products.

Criterion 15.2 – (a) Covered FIs must ensure that the risks arising from the development of new products or commercial practices or from the use of new or developing technologies are assessed "in advance" (DDA, Art. 9(2)). In the case of new technology, there is a general requirement to assess risk before it is used (FMA Guideline 2013/1, point 3.3), but this is not explicitly required in respect of new products and practices. However, as mentioned in c.15.1, new products and new business models, including new distribution mechanisms are factors that must be considered when conducting a business risk assessment.

(b) There is a general requirement for covered FIs to define effective internal control and monitoring measures to reduce risks identified in NRA II and individual business risk assessment (DDA, Art. 9a(5)). Covered FIs must assess the use of new technology and take appropriate measures to reduce risk (FMA Guideline 2013/1). There is no sufficiently clear obligation to take measures to manage and mitigate risks emanating from the risks addressed under c.15.1 in respect of new products and new business practices or developing technologies.

Criterion 15.3 – (a) Liechtenstein has conducted a risk assessment with regard to regulated TT activities (NRA-VA) on the basis of 2016 to 2019 data and information; the NRA-VA was finalised in early 2020 and an update published in August 2021. The update covers risks arising from: (i) VA activities (e.g., use of tokens to raise capital and operation of VA trading platforms); and (ii) activities or operations of VASPs. The update draws on additional sets of data not previously available (e.g., cross-border transactions, connections to countries with strategic deficiencies, and BO by country of customer base).

Analysis of VAs and the VASP sector is based on information provided by the FIU, FMA, OPP, the Office for Financial Innovation, and publicly available information. The analysis divides the market into three service categories: (i) issuance of tokens; (ii) exchange services; and (iii) other, including custody. Whilst the private sector did not contribute to the first risk assessment (on the basis that there was no regulated TT market at the time), there was close exchange with the market for the update.

Together, the original and updated NRA-VA analyse threats, vulnerabilities (inherent risk and AML/CFT compliance), and then assign residual ML and TF risk ratings: (i) exchange services – medium-high (ML and TF); (ii) other – medium (ML) and medium-high (TF); and (iii) issuance of tokens – medium-low (ML) and medium-high (TF).

(b) A risk-based approach to preventing or mitigating the ML/TF risks identified in the NRA-VA has been developed. The FMA has introduced a notification regime for those TT Service Providers that are not defined as VASPs in the FATF Recommendations, is implementing a risk-based

approach to supervision and has added additional safeguards to ensure the effective application of CDD measures. It has established a Regulatory Laboratory and FinTech Department, which, inter alia, is responsible for the registration of covered VASPs.

The FIU has purchased a Chainalysis Reactor and trained five employees in Blockchain analysis. The National Police have created an autonomous office to deal with mobile, computer and network forensics and investigation of blockchain technology and VAs, which is equipped with technical evaluation and analysis tools. One additional position in the OPP has been created, which will be responsible, amongst other things, for the investigation and prosecution of cases involving VAs.

Furthermore, the Action Plan developed on the basis of the national risk assessments also contains risk-based measures in relation to the VASP sector (see R.1).

(c) The same requirements that apply to covered FIs apply also to covered VASPs (DDA, Art. 3(1)(r) and TVTG, Art. 2(1)(k) and (m) to (q)). See c.1.10 and c.1.11.

Criterion 15.4 - (a) All legal persons established under Liechtenstein legislation and all natural persons that are resident in Liechtenstein that wish to professionally act as TT service providers must apply to be entered into the TT Service Provider Register with the FMA before beginning their activity (TVTG, Art. 12(1)). The TT Service Provider Register is held by the FMA (TTVG, Art. 43 and 23) and is available on its website (TVTG, Art. 23). As explained above, it is not clear to the AT that all VASP activities listed in the FATF definition are covered by the definition of TT Service Provider.

Since 1 April 2021, natural and legal persons representing, or distributing the services/products of a TT Service Provider established outside the country and providing TT services in and from Liechtenstein (TT agents) must be registered and subject to the DDA (TVTG, Art. 12).

(b) Covered VASPs that are legal persons are subject to similar requirements as those for covered FIs: the requirements set for natural persons (see below) must be met on an ongoing basis by: (i) members of their governing bodies; and (ii) shareholders/partners who hold a "qualifying holding" of 10% or more (TVTG, Art. 14(3)). There is no definition of "qualifying holding" in the Act, though associated legislative materials state that requirements are consistent with the provisions of financial market legislation and FMA Instruction 2020/1 to "members of the governing bodies of a TT Service Provider as well as its shareholders, owners, or partners who hold, directly or indirectly, more than 10% of the TT Service Provider". This would benefit from clarification.

In the case of a subsequent appointment or acquisition, or subsequent change in the circumstances of a member of a governing body or shareholder/partner, the FMA must be notified immediately, and its approval sought (TVTG, Art. 28(1)(a) and TVTV, Art. 6(3)). However, it is not absolutely clear that this notification must be ex ante. The FMA has no power to remove such a person, other than through withdrawal of the VASP's licence (TVTG, Art. 21(1)(a)).

A natural person is excluded from rendering a TT service if there are reasonable, serious doubts concerning their "reliability". This includes any past conviction resulting in more than three months of imprisonment or a fine of more than 180 "daily rates[46]" (TVTG, Art. 13(1)(b) and Art.

[46] A "daily rate" is a monetary penalty based on the defendant's net income. The severity of the offence is measured in the number of daily rates, with a maximum of 360 daily rates possible. The penalty is described in Art. 19 of the CC. Monetary penalties shall be assessed in daily rates. A monetary penalty shall amount to at least two daily rates. The daily rate shall be assessed in accordance with the personal circumstances and economic ability of the offender at the time of the judgement in the first instance. The daily rate shall, however, be assessed at least CHF 10 and at most CHF 1 000.

14(1)). There is also an overriding provision that allows a natural person to be excluded where there is "another reason which creates serious doubt concerning their reliability" (TVTG, Art. 14 (1)(e)). This would include the case of an associate of a natural person that is a criminal.

The FMA has the power to set aside an offence (but is not obligated to do so) if it does not believe that a person will re-offend. This could have the effect of allowing a criminal to hold an interest in a VASP, though the power has never been used and the authorities have explained that it may not be used where it could affect business operations. Nevertheless, this is not clear and would benefit from clarification.

Criterion 15.5 – The FMA takes action to identify unregistered VASP activities performed by natural or legal persons, such as systemically using reports from third parties, subscription to the trade register's RSS Feed which shows all new entries, regular exchanges with the Office for Economics whenever a person applies for a business licence in connection with crypto-services, media monitoring and subscription to newsletters and blogs in the fintech realm.

If there are indications that an activity subject to registration under the TVTG is being carried out without authorisation, the FMA initiates a clarification/determination procedure. It requests information and documents from the person concerned as if they were registered (TVTG, Art. 43) and, if this reveals that activities are being provided without registration, the FMA files a criminal complaint with the District Court (TVTG, Art. 47(1)(a)) and, as a rule, prohibits the activity with immediate effect (TVTG, Art. 43(8)).

Sanctions apply to persons who carry out unauthorised business. A natural person is liable to imprisonment for up to one year or a fine of up to 360 "daily rates". "Daily rates" are calculated by the courts based on the particular circumstances of the convicted person, with a minimum of CHF 10 and a maximum of CHF 1 000 (fine up to CHF 360 000). In the case of legal persons, these penal provisions are applied to members of management and other natural persons who acted or should have acted on the legal person's behalf. These responsible persons, together with the legal person itself, are jointly and severally liable to monetary penalties, fines, and costs (TVTG, Art. 47 and 48).

Criterion 15.6 – (a) The FMA is the supervisor for covered VASPs and for ensuring compliance with the AML/CFT framework (TVTG, Art. 39 and DDA, Art. 23). Ahead of application of a submission, an external auditor must complete a due diligence review. Ahead of registration, the due diligence "concept" of a VASP must be checked by an external auditor and registration process collects detailed information on the implementation of preventive measures, which is subject to checks by the FMA. In the first year following registration, a standard inspection (onsite visit) is performed for covered VASPs (DDO, Art. 37a (1)).

More generally, a risk-based approach to supervision is in the process of implementation. Risk data from market participants was obtained for the first time in June 2020 and again at the beginning of 2021. Based on this data and the results of the NRA-VA, the FMA will focus its activity (onsite inspections) primarily on TT exchange service providers. For other entities, a commissioned audit is carried out by an external auditor. After the initial on-site inspection, the general risk-based approach outlined under c.26.5 applies to VASPs.

(b) The FMA has a broad range of powers to supervise and monitor the compliance of covered VASPs which are the same as available for covered FIs. The FMA has the authority to conduct inspections (see c.27.2), compel the production of information (see c.27.3) and impose a range of disciplinary and financial sanctions, including withdrawal, restriction or suspension of a licence granted under "special legislation" for failure to comply with the DDA or Regulation (EU) 2015/847 (DDA, Art. 28(1) (see also c.27.4 and R.35).

Criterion 15.7 - The FMA is empowered to issue orders, guidelines, and recommendations with regard to covered VASPs (DDA, Art. 28(1)(a)). The FMA has published: (i) an instruction to assist

persons in the VASP registration process (FMA Instruction 2020/1 - Registration as a Service Provider under the TVTG); and (ii) an instruction for carrying out VA transfers ("travel rule" requirements) (FMA Instruction 2021/18). This includes a due diligence concept checklist. In addition, other FMA Instructions have sections dedicated to VASPs: (i) FMA Instruction 2018/7 on interpretation of the DDA has a special chapter for VASPs; (ii) FMA Instruction 2019/7 on remote onboarding deals mostly with the VASP sector; (iii) FMA Guideline 2013/1 on risk-based due diligence sets special requirements for VASPs. In addition, the FIU instruction on the submission of SARs/STRs contains specific requirements for VASPs.

Other guidance, specifically that related to general AML/CFT obligations, is relevant as well for the VASP sector.

As described under c.15.6, the due diligence "concept" to be applied by applicants was subject to feedback as part of the process for applying to be registered.

Criterion 15.8 - (a) Covered VASPs are subject to a range of criminal and administrative sanctions in the same manner applicable to covered FIs for breaches of their AML/CFT obligations (see c.35.1). The range of criminal sanctions that may be applied by the Princely Court for failing to report to the FIU under the DDA or violating TFS is not considered to be sufficiently proportionate.

(b) The same penal provisions apply to members of management of covered VASPs as to covered FIs (see c.35.2). In addition, Art. 48 TVTG states that the penal provisions are applicable to the members of management and other natural persons who acted or should have acted on behalf of the legal person. All persons, legal entities included, are jointly liable for monetary penalties, fines and costs.

Criterion 15.9 – Except for modifications intended to address higher risk in the TT sector, the same requirements for preventive measures that apply to covered FIs are applicable to covered VASPs - subject to qualifications (a) and (b) below.

The following modifications are relevant for addressing inherently higher TT risk: (i) very low thresholds for CDD (FMA Instruction 2018/7, chapter II – TT service provider point 5); (ii) prohibition of SDD procedures (FMA Instruction 2018/7, chapter II – TT service provider point 4); (iii) use of IT-based systems (DDA, Art. 21(1) and FMA Instruction 2018/7, chapter II - TT service provider point 6.1); (iv) additional controls for unhosted wallets (FMA Instruction 2018/7, chapter II - TT service provider points 6.7 and FMA Instruction 2021/18); (v) due diligence for high risk originating or beneficiary VASPs (FMA Instruction 2021/18; and (vi) more general CDD controls (FMA Instruction 2018/7, chapter II – TT service provider point 6.6).

(a) Covered VASPs have to conduct CDD on all business relationships and occasional transactions (with no threshold set) (DDA, Art. 5(2)(g)), with the exception of TT exchange service providers operating exclusively physical exchange machines for settlement of transactions, where the threshold for conducting CDD is CHF 1 000 or more (irrespective of whether the transaction takes place in a single operation or several between which there appears to be a connection) (DDA, Art. 5(2)(h)).

(b)(i) and (ii) The DDO applies to TT transfers between covered VASPs that exceed CHF 1 (one) (DDO, Art. 23b). Transfers are always considered to be cross-border (DDO, Art. 23b).

The following information must be collected and transmitted by the covered originating VASP: (i) the originator's name, designation[47] or number of the account, and address, number of a valid official identity document, customer number, or date and place of birth; and (ii) the beneficiary's

[47] Designation means the name, number or sequence of letters and digits of the account.

name, and designation or number of the account (DDO, Art. 23d). If a transfer does not take place from, or to, an account, a unique transaction reference can be transmitted rather than account information (DDO, Art. 23d(2)). Information on the originator must be verified by the covered originating VASP before execution of the transfer in order to ensure that it is "correct, complete and suitable" (DDO, Art. 23e)). Information must be exchanged in a secure manner prior, simultaneously, or concurrently to completion of the VA transfer (FMA Instruction 2021/18, point 4).

Whilst there is no reference in the DDO to an obligation that the covered beneficiary VASP obtain required originator information on transfers, it is required to obtain "incomplete or non-transmitted" data from the originating VASP (the effect of which is considered to be the same) (FMA Instruction 2021/18, points 4.3, 4.4 and 4.5.1). There is a requirement for the covered beneficiary VASP to obtain and verify beneficiary information (FMA Instruction 2021/18, point 4.3).

Information that is transmitted must be held by the covered originating and beneficiary VASP (DDO, Art. 27 (1)(h)). This must be always made available to the domestic authorities and courts (DDO, Art. 28(1)(c)): there is no exception in relation to a domestic wire transfer.

(b)(iii) The covered beneficiary VASP must set up effective risk-based procedures in order to determine: (i) whether to reject or suspend a VA transfer on the basis that it lacks required information (or information is not correct); and (ii) appropriate follow-up action. Where information is missing, the covered originating VASP has three days in which to submit the required and accurate information. The transfer may not be concluded without this information (DDO, Art. 23f).

Targeted financial sanctions apply to covered VASPs in the same way they do to covered FIs.

(b)(iv) The definition of VA transfer is limited to transfers between covered VASPs. However, in case of a transfer of VAs between a covered VASP and an FI, the FI must be registered as a VASP as well. Because of this, it will be a transfer between two VASPs. If the FI is located outside Liechtenstein and would be considered a TT service provider under the TVTG but can provide the service in the foreign country as an FI, the DDO must also be applied.

Criterion 15.10 - The same rules and mechanisms apply to covered VASPs as to covered FIs. Provisions in the ISA and related Ordinances do not contain exceptions with regard to VAs and VASPs.

Criterion 15.11 - The FMA is able to exchange information internationally, including information held by covered VASPs, and is able to cooperate with counterparts.

Weighting and Conclusion

There is no general regulation of transfers of VAs or provision of financial services to VA issues, which is called for by the FATF Recommendations. The authorities have explained that, instead, they regulate all persons that provide such services.

Whilst controls to prevent criminals from running or controlling VASPs are in place, where there is a subsequent change in circumstances of a person that runs or controls a VASP (e.g., they are convicted for a criminal offence), the only power available to the supervisor is to remove the VASP's registration. Notwithstanding the broad range of administrative sanctions that are available to the FMA to deal with failure to comply with AML/CFT requirements (except reporting requirements), the range of criminal sanctions that may be applied by the Princely Court for failing to report to the FIU under the DDA or violating TFS is not considered to be sufficiently proportionate. Other shortcomings are considered minor.

Given the level of development of the VASP sector in Liechtenstein (4 billion transactions volume in 2020), a higher weighting has been given to shortcomings identified under c.15.3 onwards.

Shortcomings underlined under the conclusion to R.10 with regard to the scope of application of the DDA are also relevant here.

R.15 is rated PC.

Recommendation 16 – Wire transfers

In the 4th round MER of 2014, Liechtenstein was rated C with former SR VII.

It should be noted for Liechtenstein that domestic wire transfers include any chain of wire transfers that takes place entirely within the borders of the EU and the European internal market and that the corresponding legal framework is extended to members of the EEA.

Regulation (EU) 2015/847 concerning information accompanying transfers of funds applies directly to Liechtenstein (DDA, Art.12 (1)).

Criterion 16.1 **–** (a) All cross-border wire transfers exceeding EUR 1 000 should be accompanied by the following information on the payer i.e., the originator: (i) the name of the payer; (ii) the payer's payment account number; and (iii) the payer's address, official personal document number, customer identification number, or date and place of birth. In case of a wire transfer not made from a payment account, the PSP of the payer shall ensure that the transfer is accompanied by a unique transaction identifier (Regulation (EU) 2015/847, Art. 4 (1) and (3)).

(b) All cross-border wire transfers exceeding EUR 1 000 shall be accompanied by the following information on the payee i.e., beneficiary: (i) the name of the payee; and (ii) the payee's payment account number. In case of a wire transfer not made to a payment account, the PSP of the payer shall ensure that the transfer is accompanied by a unique transaction identifier (Regulation (EU) 2015/847, Art .4 (2) and (3)).

FIs are required to undertake CDD measures when carrying out occasional transactions that are wire transfers and so the accuracy of payer information must be verified (see c.10.2). Transfers of exactly EUR 1 000 are not covered - contrary to the FATF Recommendations.

Criterion 16.2 **–** In the case of a batch file transfer from a single payer where the PSP of the payee is established outside the EEA, the batch file must contain the payer and payee information referred to under c.16.1 that is fully traceable. Individual transfers must carry the payment account number of the payer or a unique transaction identifier (Regulation (EU) 2015/847, Art. 6 (1)).

Criterion 16.3 **–** Cross-border wire transfers below EUR 1 000 must always be accompanied by: (i) the names of the payer and of the payee; and (ii) the payment account numbers of the payer and of the payee or, where Art. 4(3) applies, the unique transaction identifier information (Regulation (EU) 2015/847 (Art. 6(2)).

Criterion 16.4 **–** The PSP of the payer need not verify the information on the payer referred to in c.16.3 unless it has reasonable grounds for suspecting ML or TF (Regulation (EU) 2015/847, Art. 6 (2)).

Criterion 16.5 and 16.6 **–** Wire transfers within the EEA are considered domestic transfers for the purposes of R.16, consistent with the FATF Recommendations. Domestic transfers shall be accompanied by at least the payment account number of both the originator and the beneficiary, or by a unique transaction identifier (Regulation (EU) 2015/847 (Art. 5)).

The PSP of the payer shall, within three working days of receiving a request for information from the PSP of the payee or from an intermediary payment service provider, make available the information set out under c.16.1 or c.16.3 as appropriate (Regulation (EU) 2015/847, Art. 5 (2)).

The PSP of the payer is required to respond fully and without delay to requests for information by appropriate AML/CFT authorities (Regulation (EU) 2015/847, Art. 14).

Criterion 16.7 **–** The PSP of the payer shall retain records of all the information referred to above for a period of five years (Regulation (EU) 2015/847, Art. 16 (1)).

Criterion 16.8 **–** The PSP of the payer is not allowed to execute any transfer of funds before ensuring full compliance with Art. 4 (see requirements above) of Regulation (EU) 2015/847 without prejudice to the derogations provided for in Art. 5 and Art. 6 (transfers of funds within the EEA and transfer of funds outside of the EEA) (Regulation (EU) 2015/847, Art. 4 (6)).

Criterion 16.9 **–** The intermediary PSP shall ensure that all the information received on the payer and the payee that accompanies a transfer of funds is retained with the transfer (Regulation (EU) 2015/847, Art. 10).

Criterion 16.10 **–** No exemption is provided by Regulation (EU) 2015/847 concerning technical limitations that prevent the appropriate implementation of the requirements on domestic wire transfers.

Criterion 16.11 **–** The intermediary PSP is required to implement effective procedures including, where appropriate, ex-post or real-time monitoring, in order to detect whether required payer or required payee information in a transfer of funds is missing (Regulation (EU) 2015/847, Art. 11 (1)).

Criterion 16.12 **–** The intermediary PSP shall establish effective risk-based procedures for: (i) determining whether to execute, reject or suspend a transfer of funds lacking the required payer and payee information; and (ii) taking the appropriate follow up action (Regulation (EU) 2015/847 (Art. 12(1)). In the case of repeated failures, it must report those failures and the steps taken to address them to the competent supervisory authority (Regulation (EU) 2015/847 (Art. 12(2)).

PSPs (and IPSPs) are required to establish and maintain effective policies and procedures to comply with the Regulation. These policies and procedures should be proportionate to the nature, size and complexity of the PSP's or IPSP's business, and commensurate with the ML/TF risk to which the PSP or IPSP is exposed (ESAs' Joint Guidelines to prevent the abuse of funds transfers for ML/TF purposes, point 18).

Criterion 16.13 **–** The PSP of the payee shall implement effective procedures, including, where appropriate, ex-post monitoring or real-time monitoring, in order to detect whether the information on the payer or the payee is missing in a cross-border wire transfer (Regulation (EU) 2015/847, Art. 7(2)).

Criterion 16.14 **–** In the case of transfers of funds exceeding EUR 1 000, the beneficiary FI must verify the accuracy of the identification information on the beneficiary before crediting their payment account or making the funds available to the payee (Regulation (EU) 2015/847, Art. 7(3)), as described under the analysis for c.16.7. The PSP of the payee shall retain records of all the information referred to above for a period of five years (Regulation (EU) 2015/847, Art. 16 (1)).

Transfers of exactly EUR 1 000 are not covered - contrary to the FATF Recommendations.

Criterion 16.15 **–** The beneficiary FI is obligated to implement effective risk-based procedures for determining whether to execute, reject or suspend a transfer of funds lacking the required originator and beneficiary information and for taking the appropriate follow-up action

(Regulation (EU) 2015/847, Art. 8). The same reporting obligations outlined under c.16.12 also apply.

Criterion 16.16 **–** Regulation (EU) 2015/847 applies to all kinds of payment service providers the transfers of funds, in any currency, which are sent or received by an ordering, intermediary or beneficiary FI established in the EEA. The term "payment service provider" comprises the categories of payment service provider referred to in Art. 1(1) of Directive 2007/64/EC which includes money or value transfer services.

PSPs with a licence under the Payment Service Act are subject to due diligence requirements (DDA, Art. 3 (1) (h)). Liechtenstein branches, agents and representative offices of foreign PSPs are also subject to due diligence requirements (DDA, Art. 3 (2)).

Criterion 16.17 **–** (a) The PSP shall take into account missing information on the originator or the beneficiary in order to determine whether an SAR/STR is to be filed (Regulation (EU) 2015/847, Art. 13).

(b) Regulation (EU) 2015/847 does not require a SAR/STR to be filed in each country affected by the suspicious wire transfer or to make relevant transaction information available. However, given the principle of territoriality of AML/CFT Laws, when a PSP is established in several countries, performs a money transfer between two of its entities, and the transaction proves to be suspicious, it may be required to submit a SAR/STR to the FIU in each of these countries pursuant to their respective domestic laws. EU Directive 2015/849 requires compliance officers to file a SAR/STR with the FIU of the Member State in whose territory the obliged entity with suspicion is established.

Criterion 16.18 **–** FIs conducting wire transfers are subject to the requirements of UNSCRs 1267, 1373, and successor resolutions. Such a requirement is provided for in the ISA (Art. 2c (2)) and the freezing obligation is stipulated in the Terrorism Ordinance, the Taliban Ordinance and the ISIL/Al-Qaida Ordinance.

Weighting and Conclusion

There are no shortcomings.

R.16 is rated C.

Recommendation 17 – Reliance on third parties

In the 4th round MER of 2014, Liechtenstein was rated LC on R.9. Countries where third party could be located were determined without an assessment by the Liechtenstein authorities of the supervisory framework and of the CDD measures in place in the concerned countries. There was no restriction on placing reliance on countries that did not have a satisfactory supervisory framework and CDD measures.

The authorities have suggested that provisions under the DDA (delegation of CDD) cannot be considered as third-party reliance within the meaning of R.17 and should rather be regarded as outsourcing arrangements (that are not covered by R.17). This is because R.17 permits copies of identification data and other relevant CDD documentation to be provided by the relied-on party upon request by the relying party, whereas the DDA requires this data and documentation to be immediately obtained (at the time that necessary information concerning elements (a) to (c) of R.10 are obtained). The AT does not agree with this since, in its view: (i) the requirement to immediately call for data and relevant documentation is one of a number of steps that could be taken to be satisfied that data will be made available without delay (c.17.1(b)); and (ii) CDD conducted by the relied on party is not based on instructions issued by the relying party (normally

the case for outsourcing) and, instead, the relied on party applies its own measures (in line with the DDA, Directive (EU) 2015/849 or equivalent).

In addition, it should be mentioned that the DDO separately deals with: (i) delegation of due diligence (Art. 24); and (ii) outsourcing arrangements for ongoing monitoring (Art. 24a), with different requirements applying in each case. In addition: (i) existing requirements for delegation of CDD are based substantially on the requirements of R.17; (ii) Art. 14(4) of the DDA states that delegation provisions do not apply to outsourcing or representation arrangements; and (iii) FMA Instruction (2018/7) on sector specific interpretation of the CDD, highlights a clear distinction between outsourcing and delegation (Art. 8.2).

Criterion 17.1 - Covered FIs can delegate due diligence measures (identification and verification of the identity of the customer, the BO, or the establishment of a customer's business profile) to another person (DDA, Art. 14 and DDO, Art. 24). The ultimate responsibility to comply with due diligence requirements remains with the covered FI delegating CDD (DDA, Art. 14(2)).

(a) and (b) - A covered FI is required to ensure that the delegate obtains or issues information and documentation in accordance with the provisions of the DDA and DDO and transmits them immediately to the covered FI (DDO, Art. 24(1)).

(c) The delegate must be subject to due diligence under the DDA, or a natural or legal person domiciled in another EEA member state or third country: (i) whose due diligence and record keeping requirements meet Directive (EU) 2015/849 (which is not entirely in line with c.17.1(c) which refers to compliance with R.10 and R.11); (ii) whose compliance is supervised consistently with Directive (EU) 2015/849; and (iii) who is not domiciled in a state with strategic deficiencies (DDA. Art. 14 (1)). The covered FI is required to assess case by case whether the delegate is an obliged entity and subject to AML/CFT supervision (FMA Instruction 2017/7). In this respect, the FMA publishes an exhaustive list of third countries that can be considered to have: (i) CDD and record-keeping requirements; and (ii) a supervisory regime in place equivalent to those under Directive (EU) 2015/849.

The provision of "joint services" set out in Art. 15(1) of the DDA can also be considered as a form of "reliance on third parties". It is permissible for different covered FIs that operate using the same business name to nominate one amongst them (who will hold the "mandate") to be responsible for application of the due diligence measures referred to in Art. 5(1) of the DDA in respect of a particular shared customer. In this situation, persons subject to the DDA who do not personally conduct the CDD, shall: (i) ensure that they are granted access at any time to the due diligence files held by the mandate holder - on request (DDA, Art. 15(3)(a)); and (ii) monitor the proper performance of the due diligence obligations by the holder of the mandate (DDA, Art. 15(3)(b)), performance of which has to be documented in a written agreement. Art. 15(1) can only be applied by respective domestic persons who are subject to the DDA, thus the person holding the mandate will be subject to an obligation to have measures in place for compliance with CDD and record-keeping requirements in line with R.10 and R.11 and supervised for compliance therewith. Whilst Art. 15(1) does not specifically require that CDD information be obtained immediately, this is the effect of Art. 5(1) to which those placing reliance remain subject.

Criterion 17.2 – The FMA list of third countries (see c.17.1(c)) whose requirements for CDD, record keeping, and supervision are considered to meet Directive (EU) 2015/849 must be based on AML/CFT assessments of international agencies (DDA Art. 14(3)). The FMA has listed 13 countries outside the EEA as countries with AML/CFT measures equivalent to those under the Directive. The list is drawn up by the FMA based on information provided in the latest mutual evaluation or follow-up reports available (i.e., FATF, MONEYVAL. etc) for the countries

concerned. Whilst the FMA assessment does not consider country risk more generally, as noted under c.17.1, covered FIs are prohibited from delegating due diligence measures to a person who is domiciled in a state with strategic deficiencies. Further, whilst there is no general requirement for the FMA to take account of information on ML/TF risks in the countries listed, the source for the list of 13 countries is MERs in which country risk is addressed. Accordingly, this shortcoming can be assessed as a minor.

Criterion 17.3 - In a case of delegation to group member, alternative provisions may be applied.

(a) Where group provisions are applied, CDD, record-keeping and internal organisation requirements must be consistent with Directive (EU) 2015/849 (which is not entirely in line with c.17.3(a) which refers to compliance with R.10 to R.12 and R.18).

(b) Where group provisions are applied, effective implementation of the above requirements must be monitored at group level by a competent authority.

(c) Where group provisions are applied, that there is no requirement for higher country risk to be adequately mitigated by the group's AML/CFT policies (the effect of which is considered to be minor). However, as explained above, the FMA has listed only 13 countries outside the EEA to which CDD may be delegated.

Weighting and Conclusion

The benchmark for determining in which countries delegates may be based is linked to compliance with elements of Directive (EU) 2015/849 rather than the more general level of country risk. This shortcoming is mitigated by a prohibition on placing reliance on countries with strategic deficiencies and use of MERs to draw up the list. Other shortcomings are minor.

R.17 is rated LC.

Recommendation 18 – Internal controls and foreign branches and subsidiaries

In the 4th round MER of 2014, Liechtenstein was rated LC on R.15. There were no requirements for FIs to screen for probity when hiring new employees and no express requirement for FIs to maintain adequately resourced the requisite internal audit function.

The introduction to R.10 lists activities to which the DDA does not apply.

Criterion 18.1 - Covered FIs are required to take necessary organisational measures and provide appropriate internal instruments of control and monitoring related to AML/CFT. In particular, FIs have to issue internal instructions, arrange secure storage of CDD files and arrange for training and development of their staff (DDA. Art. 21 (1)). Internal instructions must set out how DDA and DDO obligations are to be met in practice through appropriate policies, procedures, and controls (DDO, Art. 31(1)). As appropriate to circumstances and individual risks, internal organisation shall be designed according to the type and size of the enterprise as well as according to the number, type, and complexity of business relationships. The effective fulfilment of the internal functions and due diligence requirements must be guaranteed at all times (DDA, Art. 21 (2)).

a) Covered FIs shall appoint: (i) a compliance officer (to support and advise the executive body); and (ii) a member of the executive body to be responsible for ensuring compliance with the DDA and DDO (DDA, Art. 22(1) and DDO, Art. 34)). Whilst there is no requirement for the compliance officer to be appointed at management level, as noted, a member of the executive body has

responsibility for compliance. Internal instructions must regulate the duties and responsibilities of the compliance officer (DDO, Art. 31(2)(a)).

b) Covered FIs shall issue internal instructions that regulate appropriate verification procedures to be used in the recruitment of new employees in order to guarantee high standards, with reference to their reliability and integrity (DDO, Art. 31(2)(k)).

c) Internal instructions shall regulate the main features of the training and development of employees performing activities relevant to due diligence (DDO. Art. 31(2)(h)). Additionally, covered FIs are required to make provision for on-going, comprehensive training and development of employees performing activities relevant to due diligence (DDO, Art. 32). The process of the training shall be planned and monitored by the compliance officer (DDO, Art. 34(c)). It is explained that employees performing activities relevant to due diligence includes first, second and third lines of defence, i.e., customer facing staff, compliance staff and the investigating officer (FMA Instruction 2018/7).

d) Covered FIs are required to have an internal auditor ("investigating officer") who shall ensure compliance with the DDA, DDO and internal instructions (DDA, Art. 22 and DDO, Art. 35). In order to do so, the investigating officer shall conduct internal inspections to achieve this and report to the compliance officer and executive management (DDO, Art. 35). Internal instructions must regulate the duties and responsibilities of the investigating officer (DDO, Art. 31(2)(gbis)).

Criterion 18.2 - Covered FIs belonging to a group shall establish strategies and procedures applicable to the entire group, including data protection strategies and procedures for exchange of information within the group, for the purpose of prevention of ML, organised crime, and FT. These strategies and procedures must be effectively implemented by branches, agents, representative offices and majority-owned subsidiaries (DDA, Art. 16(1)). It is also specified that group wide policies and procedures should extend to the appointment of (a) compliance officer(s) for ensuring compliance with group policies and procedures, screening of staff, training of staff, and appointment of an independent internal audit department (DDO, Art. 25(1)(d) and (e)).

a) Covered FIs (parent entities) are required to establish policies and procedures applicable to the entire group, including procedures for exchange of information within the group, for the purpose of prevention of ML, organised crime, and TF (DDA, Art. 16 (1) and DDO, Art. 25(1)). This is considered wide enough to include CDD and ML/TF risk management.

b) Covered FIs (parent entities) shall, for the purpose of monitoring the risks associated with ML, organised crime, and FT, ensure that the persons or specialist units responsible for compliance with strategies and procedures, the internal audit department, and the external auditors of the group have access to prescribed information, including personal data, in all group companies (DDO, Art. 25(1)(a)). The reference to persons or specialist units is considered wide enough to cover compliance and AML/CFT functions. Prescribed information is: (i) information about business relationships and transactions, including investigations under Art. 9(3) and (4) of the DDA; (ii) information transmitted together with a report of suspicion, unless otherwise instructed by a financial intelligence unit; and (iii) other information required for compliance with due diligence obligations and the verification thereof as well as AML/CFT risk management. Persons subject to the DDA forming part of a domestic or foreign group (subsidiaries and branches) must grant the persons or specialist units responsible for compliance with the policies and procedures to be applied at group level, the internal audit department, and the external auditors of the group access to this prescribed information - to the extent this is necessary for global application of the due diligence standard (DDO, Art. 25(2)). Provision is made also for group companies to receive the same prescribed information (DDO, Art. 25(1)(c)).

c) The policies and procedures that covered FIs (parent entities) are required to establish must ensure the confidentiality of data that is exchanged, including safeguards to present tipping off

(DDO, Art. 25(1)(dbis). As referred to in (b) above, information may be used for specified purposes only.

Criterion 18.3 - In third countries (excluding EEA member states) in which the minimum requirements with reference to the prevention of ML, organised crime and TF are less stringent than those provided under the DDA, covered FIs shall adjust their group-wide strategies and procedures in order to follow the minimum requirements under the DDA, insofar as this is permitted under the foreign law (DDA, Art. 16 (1)). This requirement does not apply to: (i) EEA member states, notwithstanding that the DDA may set measures additional to those applied in EU Directives; or (ii) requirements set in the DDO and other enforceable means (e.g., FMA Instructions).

If, due to restrictions under the law of the other country, branches and majority-owned subsidiaries located in a third country are unable to comply with the measures required under the DDA, the covered FI must inform the FMA. In such a case the covered FI shall take additional measures to effectively address the risk of ML, organised crime and FT. If these additional measures are inadequate, the FMA may use measures such as prohibiting transactions in the third country concerned or requiring the group to cease business in the country concerned (DDA, Art. 16(3)).

In case of EEA member states, there is a general assumption that these have AML/CFT measures consistent with the 4th AMLD. However, such an approach does not recognise that there may be delays or gaps in transposition and it should not be assumed that all EU members have implemented the same minimum requirements as defined in the DDA. This approach is not fully in line with c.18.3.

Weighting and Conclusion

Requirements dealing with host countries with less strict AML/CFT requirements only apply in the case of non-EEA member states. Shortcomings underlined under the conclusion to R.10 with regard to the scope of application of the DDA are also relevant here.

R.18 is rated LC.

Recommendation 19 – Higher-risk countries

In the 4th round MER of 2014, Liechtenstein was rated LC on R.21 since the DDA did not require EDD with respect to persons from (as opposed to in) high risk countries and there was not a sufficiently broad power to issue and enforce countermeasures in relation to transactions or business relationships involving high risk countries.

"States with strategic deficiencies" are those states whose national systems for the prevention of ML and TF exhibit strategic deficiencies that pose significant threats to the financial system pursuant to: (i) delegated acts of the European Commission referred to in Art. 9(2) of Directive (EU) 2015/849; or (ii) assessments by international organisations (including the FATF) established to prevent ML and TF (DDA, Art. 2(1)(u)). The delegated acts of the Commission were last updated on 7 May 2020 and list 20 high-risk third countries. The Government may also, notwithstanding delegated acts of the Commission, identify additional states with strategic deficiencies on the basis of evaluations of international organisations, e.g., the FATF (DDA, Art. 11a(6)(a)). Countries with strategic deficiencies are listed in the DDO (Annex 4). The list includes both the Democratic People's Republic of Korea and Iran.

The introduction to R.10 lists activities to which the DDA does not apply.

Criterion 19.1 - With regard to business relationships or transactions involving states with strategic deficiencies, covered FIs shall apply EDD as set out in Annex 2, Section B and under Art. 11 (DDA, Art. 11a(1)). This includes those subject to a call from the FATF to apply enhance measures, but such a requirement is not automatic and is dependent upon Government designation. This deficiency is considered to be minor given that Government policy is to designate those countries subject to such a call and limited number of such calls during the period under review. There is no explicit requirement for the measures selected to be proportionate to the risks, but the cumulative application of additional measures listed under DDA Annex 2 Section B as examples is intended to have that effect.

Covered FIs are prohibited to delegate due diligence to a person domiciled in states with strategic deficiencies (DDA, Art. 14(1)(b)(3)) and outsourcing is prohibited to providers domiciled in states with strategic deficiencies (DDO, Art. 24a(1a)(e)). Also, during a correspondent relationship, if the intragroup respondent institution is located in a state with strategic deficiencies, further additional measures must always be applied (FMA RBA guideline, Art. 5.8.3).

Criterion 19.2 - With regard to business relationships or transactions involving states with strategic deficiencies, the Government may prescribe by ordinance that one or more of the following risk-reducing measures be taken: (i) application of additional EDD measures; (ii) introduction of enhanced relevant reporting mechanisms or a systematic reporting obligation for financial transactions; and (iii) restriction of business relations or transactions with natural persons or legal entities (DDA, Art. 11a(2)). More generally, by ordinance, the Government may also: (i) prevent the establishment of subsidiaries, branches or representative offices in Liechtenstein; (ii) introduce a ban on covered FIs establishing subsidiaries, branches or representative offices; (iii) apply enhanced supervisory measures for subsidiaries or branches; (iv) introduce stricter requirements for the external review of subsidiaries and branches of covered FIs; and (v) introduce an obligation to review, change or, if necessary, terminate correspondent banking relationships (DDA, Art. 11a(3)).

Additionally, the Government may: (i) notwithstanding the delegated acts of the European Commission and on the basis of evaluations of international AML/CFT agencies, identify additional states with strategic deficiencies; and (ii) establish reporting or licensing requirements for business relationships and transactions (DDA, Art. 11a(6)).

Criterion 19.3 - Countries with strategic deficiencies are listed in the DDO (Annex 4). As the amendment of Annex 4 (list of states with strategic deficiencies) requires a revision of the DDO, the change of the law has to be announced in the Liechtenstein Legal Gazette – publication body for all legal provisions. Additionally, every update to the list of states with strategic deficiencies is also communicated to covered FIs through the FMA newsletter and website.

Weighting and Conclusion

There is only one minor shortcoming. However, shortcomings underlined under the conclusion to R.10 with regard to the scope of application of the DDA are also relevant here.

R.19 is rated LC.

Recommendation 20 – Reporting of suspicious transaction

Liechtenstein was rated largely compliant with the previous R.13 and SR.IV. For both Recommendations, shortcomings were identified only with regard to their effective implementation.

The introduction to R.10 lists activities to which the DDA does not apply.

Criterion 20.1 - Where suspicion of ML, a predicate offence to ML, organised crime and TF exists, FIs must immediately submit a report to the FIU in writing (DDA, Art. 17). Further to this requirement, the Guidance for submitting SARs/STRs to the FIU under Art. 17 of the DDA (hereinafter: FIU Guidance) stipulates, that there are no special preconditions in this regard (such as a "justified suspicion"). A suspicion requires that indicia or facts exist from which the suspicious situation can be inferred in a comprehensible and objective way. The FIU guidance provides a list of constellations that give rise to a report of suspicion and this list is not exhaustive.

Persons subject to the DDA may not execute transactions in respect of which there is an obligation to report suspicions, until such a report has been submitted, except when an advance-notification is not possible or would frustrate the efforts to pursue the person. In this case reports may exceptionally be submitted immediately after the transaction has been executed (DDA, Art. 18). A reporting obligation is also set for the supervisory authorities and all offices of the National Administration (DDA, Art. 17(1))***.***

Criterion 20.2 – The laws provide for a general obligation to report suspicions without specifically mentioning the obligation to report on transactions. The FIU Guidance stipulates that the reporting obligation also exists if a business relationship has not yet been established or if the transaction has not yet been executed. Thus, the obligation under Art. 17 DDA is not only applicable in the context of executed transaction but expands to attempted transactions, including all circumstances concerning the relationship with a customer, regardless of the type of suspicion or amount of funds. No restrictions exist as to the amount of the transaction.

Weighting and Conclusion

Shortcomings underlined under the conclusion to R.10 with regard to the scope of application of the DDA are also relevant here.

R.20 is rated LC.

Recommendation 21 – Tipping-off and confidentiality

Liechtenstein was rated largely compliant with the previous R.14. The remaining concern was related to the tipping-off prohibition which did not apply to information related to a SAR/STR.

Requirements set out in the DDA and DDO with regard to countries with strategic deficiencies do not directly apply to insurance agents and institutions exclusively operating in the field of occupational old age, disability, and survivors' provision which, according to FMA instruction (2018/7) on the sector specific interpretation of the DDA, primarily include pension schemes under the Occupational Pension Act and pension funds under the Pension Funds Act. T

Criterion 21.1 **-** Persons subject to the DDA, the supervisory authorities and the offices of the National Administration and their executive bodies and employees, who submit a report to the FIU, shall be released from any civil and criminal liability, if this report is proven to be unjustified, provided that they did not act deliberately. (DDA, Art. 19(1)). While the legislation provides for the protection of executive bodies and employees, it is not clear whether the definition of 'executive bodies' extends also to directors and officers.

Criterion 21.2 - Persons subject to the DDA, as well as their executive bodies and employees, may not inform the contracting party, the BO, or third parties, with the exception of the supervisory authorities or the competent prosecution authorities, that they a) are submitting, have submitted or intend to submit a report to the FIU or b) have received instructions from the FIU on suspending the execution of a current transaction that might be connected with ML, predicate

offences to ML, organised crime or TF. (DDA, Art. 18b (1)). FIU guidance stipulates, that this ban on disclosure under the DDA is not limited in time.

The law refers only to employees and remains silent with regard to directors and officers, although it is assumed that directors are covered through 'executive bodies'.

This confidentiality provision does not apply to information-sharing between: (i) FIs, their branches and subsidiary undertakings; and (ii) FIs and institutions from third countries, in which requirements equivalent to those of Directive (EU) 2015/849, in cases referring to the same client and the same transaction and in which two or more persons subject to the DDA are involved. (DDA, Art. 18b (3)).

Weighting and Conclusion

Financial institutions and their executive bodies and employees are protected by law from both criminal and civil liability, in cases if suspicion report should prove to be unjustified and provided that they did not act deliberately. They also may not inform third parties on the fact that an SAR/STR is being filed with FIU. While it is assumed that directors and officers are covered with executive bodies, the definition of executive bodies is not provided in the legislation.

R.21 is rated LC.

Recommendation 22 – DNFBPs: Customer due diligence

In the 4th round MER of 2014, Liechtenstein was rated PC on R.12. The assessors identified a wide range of deficiencies regarding CDD measures in place for different types of DNFBPs.

In addition to DNFBPs covered by the FATF Recommendations, section 1.4.4 lists additional activities that are subject to the DDA. These additional areas of regulation are based on the EU AMLDs and are not linked to particular risks identified in Liechtenstein. Later references to "covered DNFBPs" (and in R.23) exclude these businesses and professions.

Criterion 22.1 - Covered DNFBPs have an obligation to comply with CDD requirements in the circumstances set out under c.10.2 (DDA, Art. 5(2)(a) to (d)).

a) In addition, CDD measures shall be performed by casinos in connection with cashing of winnings or making of stakes, or with both, to the value of CHF 2 000 or more, irrespective of whether the transaction is carried out in a single operation or in several operations which appear to be linked (DDA, Art. 3(1)(l) and Art. 5(2)(f)). Obligations to comply with CDD requirements are also set out in the Casino Ordinance[48], where casinos (but not internet-based casinos) have to apply CDD when: (i) they establish a business relationship, such as opening a chip custody account or a guest account (Casino Ordinance, Art. 136); (ii) they carry out an occasional transaction of CHF 2 000 or more, including exchanges of domination, foreign currency and other cash transactions (Casino Ordinance, Art. 135); and (iii) a withdrawal is made from a guest account (Casino Ordinance, Art. 152(2)).

b) CDD measures shall be performed by real estate agents, insofar as their activities cover the purchase or sale of real estate (DDA, Art. 3(1)(p)).

c) CDD measures shall be performed by DPMS for occasional transactions in cash amounting to CHF 10 000 or more, irrespective of whether the transaction is carried out in a single operation or in several operations which appear to be linked (DDA, Art. 3(1)(q) and 5(2)(e)).

[48] AML/CFT requirements applicable to internet-based casinos are set out in the Ordinance on Online Gambling.

d) CDD measures shall be performed by lawyers with an authorisation under the Lawyers Act, as well as legal agents as referred to in Art. 108 of the Lawyers Act insofar as they provide tax advice to their clients or assist in the planning and execution of financial or real estate transactions concerning the following: (i) buying and selling of undertakings or real estate; (ii) management of client funds, securities or other assets of the client; (iii) opening or management of accounts, custody accounts or safe deposit boxes; and (iv) procurement of contributions necessary for the creation, operation or management of legal entities (DDA, Art. 5(2)(a) to (d)). Provisions in respect of legal services do not apply to preparing clients for transactions with respect to the creation, operation or management of legal persons or arrangements. This is considered to be only a minor shortcoming given that the service is generally provided under the umbrella of a TCSP engaged in establishing legal persons or trusts.

CDD measures shall be performed by accountants insofar as they assist clients in the planning and execution of financial or real estate transactions listed above. This excludes preparing clients for transactions in respect of the creation, operation or management of legal persons or arrangements. This is considered to be only a minor shortcoming given that the service is generally provided under the umbrella of a TCSP engaged in establishing legal persons or trusts.

Notaries may neither provide general legal advice, nor assist in the sale and purchase of real estate. Furthermore, the authority to act as a notary does not entail the permission to hold or manage money or other assets on behalf of clients. However, notarisations and certifications may be provided for customers in connection with real estate transactions or the creation of legal entities, which is considered to be within the scope of c.22.1(d)).

e) CDD measures shall be performed by TCSPs in the circumstances set out under c.10.2 where one of the following services is provided on a professional basis for the account of third parties: (i) establishment of companies or other legal entities; (ii) performance of the management or executive function of a company, the function of partner in a partnership or a comparable function in another legal person or appointment of another person for the afore-mentioned functions; (iii) provision of a registered office, a business, postal or administrative address and other related services for a legal entity; (iv) performance of the function of a member of a foundation board of a foundation, trustees of a trust or a similar legal entity or appointment of another person for the afore-mentioned functions; or (v) performance of the function of nominee shareholder for another person, where the company concerned is not listed on a regulated market and subject to the disclosure requirements in conformity with EEA law or similar international standards, or appointment of another person for the afore-mentioned functions. This sub-criterion is not fully in line with the FATF Recommendations, as Criterion 22.1 (e) does not provide for the possibility not to conduct CDD during the performance of the function of nominee shareholder if the company is listed on a regulated market and is subject to disclosure requirements in conformity with EEA law or similar international standards.

Requirements and shortcomings described in the DDA and DDO for covered FIs under R.10 are equally applicable to covered DNFBPs.

Criterion 22.2 - Requirements and shortcomings described in the DDA and DDO for covered FIs under R.11 are equally applicable to covered DNFBPs.

Criterion 22.3 - Requirements and shortcomings described in the DDA and DDO for covered FIs under R.12 are equally applicable to covered DNFBPs**.**

Criterion 22.4 – Requirements and shortcomings described for covered FIs under R.15 are equally applicable to covered DNFBPs.

Criterion 22.5 – Requirements and shortcomings described in the DDA and DDO for covered FIs under R.17 are equally applicable to covered DNFBPs, except that alternative provisions do not apply to DNFBP groups (DDO, Art. 24 (4)) and for the provision of "joint services", where an additional provision applies (DDA, Art. 15(2)).

The provision of "joint services" set out in Art. 15(2) of the DDA can also be considered as a form of "reliance on third parties". It is permissible for a group of board members or partners of a legal person that act by way of business (as a TCSP) to nominate one amongst them (who will hold the "mandate") to be responsible for application of the due diligence measures referred to in Art. 5(1) of the DDA to that legal person on their behalf. In this situation, persons subject to the DDA who do not personally conduct the CDD, shall: (i) ensure that they are granted access at any time to the due diligence files held by the mandate holder - on request (DDA, Art. 15(3)(a); (ii) monitor the proper performance of the due diligence obligations by the holder of the mandate (DDA, Art. 15(3)(b)), performance of which has to be documented in a written agreement (DDA, Art. 15(3)(a)); and (iii) remain responsible for compliance with their own separate CDD obligations (DDA, Art. 15(2)). Art. 15(2) can only be applied by respective domestic persons who are subject to the DDA, thus the person holding the mandate will be subject to an obligation to have measures in place for compliance with CDD and record-keeping requirements in line with R.10 and R.11 and supervised for compliance therewith. Whilst Art. 15(2) does not specifically require that CDD information be obtained immediately, this is the effect of Art. 5(1) to which those placing reliance remain subject.

Weighting and Conclusion

There are some shortcomings in the scope of application of CDD measures to DNFBPs, in particular provisions in respect of legal and accounting services. However, these shortcomings are considered to be minor, given that both are generally provided under the umbrella of a TCSP. Also, shortcomings identified in relation to FIs under R.10, 11, 12, 15 and 17 are also relevant for DNFBPs.

R.22 is rated LC.

Recommendation 23 – DNFBPs: Other measures

In the 4th round MER of 2012, Liechtenstein was rated C on R.16.

There are some shortcomings in the scope of application of CDD measures to DNFBPs. In particular provisions in respect of legal and accounting services do not apply to preparation for transactions related to the creation, operation or management of legal persons or arrangements. See R.22.

Criterion 23.1 – Covered DNFPBs have an obligation to immediately report to the FIU where there is suspicion of ML, a predicate offence related to ML, organised crime, or TF (DDA, Art. 17(2)).

Lawyers, law firms and legal agents as well as auditors, auditing companies and audit offices shall not be required to report to the FIU if they have received the information concerned in privileged circumstances, i.e.: (i) from or through a client when they are endeavouring to ascertain the legal position on behalf of their client; or (ii) in their capacity as defence counsel or representative of that client in, or concerning, judicial proceedings, including advice on instituting or avoiding proceedings, whether such information is received before, during, or after such proceedings

((DDA, Art. 17(2)). Since the reporting exemption applies only in privileged circumstances, it does not cover information collected by lawyers, law firms or legal agents under requirements set out in the DDA. The exemption does not apply to members of tax consultancy professions.

Criterion 23.2 - Requirements and shortcomings described in the DDA and DDO for covered FIs under R.18 are equally applicable to covered DNFBPs, except that there is no requirement to establish group strategies and procedures (DDA, Art. 16 (1)). Since application of R.18 to DNFBPs had not been clarified by the FATF at the time of the on-site visit, c.18.2 has been treated as not applying to DNFBPs.

Criterion 23.3 - Requirements and shortcomings described in the DDA for covered FIs under R.19 are equally applicable to covered DNFBPs**.**

Criterion 23.4 – Covered DNFBPs are subject to the same requirements regarding tipping off and confidentiality as covered FIs. Thus, the analysis under R.21 applies.

Weighting and Conclusion

Minor deficiencies have been identified in R.18, R.19 and R.21, which are equally relevant to DNFBPs. Shortcomings underlined under R.22 with regard to the scope of application of the DDA are also relevant here.

R.23 is rated LC.

Recommendation 24 – Transparency and beneficial ownership of legal persons

Liechtenstein was rated PC in 2014. The report noted that the system in place at that time did not ensure adequate transparency on BO of legal persons and did not always allow access in a timely fashion to adequate, accurate and current information on the BO of legal persons. Further, the powers of the FMA to access information were restricted to supervisory functions and the measures in place for bearer shares were not adequate.

Since then, the FATF Recommendations have changed substantially and the legal framework in Liechtenstein has developed considerably.

Criterion 24.1 - For the purpose of R.24, the following types of legal persons (group A) are relevant (in order of use):

- Foundation (PGR, Art. 552(1) to (41))
- Anstalt (Establishment) (PGR, Art. 534 to 551)
- Public limited company (PGR, Art. 261 to 366)
- Trust enterprise (PGR, Art. 932a (1) to (170))
- Limited liability company (PGR, Art. 389 to 427)
- Association (PGR, Art. 246 to 260)
- Limited partnership (PGR, Art. 733 to 755)
- Cooperative society (PGR, Art. 428 to 495)
- General partnership (open partnership) (PGR, Art. 689 to 732) (also known as "collective society")
- European company (SCE Act, SE-VO, Art. 15 and PGR, Art. 261 to 366)
- European cooperative society (SE Act, SCE-VO, Art. 17 and PGR, Art. 428 to 495)
- Partnership limited by shares (PGR, Art. 368 to 374)
- European Economic Interest Grouping (EWIVG, Art. 2, EWIV-VO and PGR, Art. 689 to 732)

The following legal persons (group B) are also available under Liechtenstein law for specific and limited purposes but, to date, have not been registered in the Commercial Register:

- Company limited by units (trade unions) (PGR, Art. 375 to 388)
- Mutual insurance associations (PGR, Art. 496 to 530)
- Auxiliary funds (linked to mutual insurance) (PGR, Art. 531 to 533)
- Unregistered partnership (PGR, Art. 680 to 688)
- Community of property (linked to inheritance) (PGR, Art. 779 to 793)

In addition, the following legal persons (group C) that are available in Liechtenstein for specific and limited purposes are not obliged to register:

- Public service undertakings (PGR, Art. 571 to 589)
- Consortium (form of joint venture) (PGR, Art. 756 to 767)
- Silent partnership (legal person with limited participation by partners) (PGR, Art. 768 to 778)
- Homesteads and entailed estates (preservation of real estate) (PGR, Art. 794 to 833)
- Simple community of rights (form of joint venture) (PGR, Art. 933 to 943)

Group C legal persons are not used in practice.

The different types, forms and basic features of legal persons are set out in the PGR and other legislation (in the sections as specified above). In addition, information is publicly available by way of factsheets on the Office of Justice website for relevant registered legal person, that describe, inter alia, what is required for formation and registration, documents to be submitted (including description of content) and fees to be paid. In relation to obtaining and recording information, relevant legal provisions can be found in the PGR and Commercial Register Ordinance (basic information), and DDA, DDO and FMA guidelines and communications (with respect to the processes for obtaining and recording BO information by persons subject to the DDA (e.g., FMA Communication 2015/7 and FMA Guideline 2018/7)). Factsheets, explanatory cases and other relevant documents and guidance regarding the central BO register are published.

Criterion 24.2 - The authorities have conducted a specific assessment of the ML risks associated with group A legal persons (and legal arrangements). This exercise began in 2019 and the report was finalised in May 2020 (Analysis of money laundering risks of Liechtenstein entities).

Separately, the authorities have conducted a national TF risk assessment that was finalised and adopted in May 2020. This included analysis of TF risks associated with Liechtenstein legal persons and legal arrangements, focussing on identified links to higher risk countries. See section 7.2.2 of the MER. There was, however, no consideration of: (i) except for NPOs, the inherent vulnerabilities for TF purposes of all the different types of legal persons and arrangements (since the authorities consider that, irrespective of form, all could be misused in the same way); or (ii) their activities (except for NPOs – subject to a separate risk assessment).

Criterion 24.3 - All the legal persons specified above are subject to mandatory registration with the Office of Justice, with the exception in group A of: (i) some associations, some cooperative societies, and most "private-benefit" foundations (8 693 as of 31 December 2020); and (ii) group C legal persons.

The register is maintained by the Commercial Register Division (a department of the Office of Justice) and the information held on the public record includes (inter alia): (i) name; (ii) legal form; (iii) date of incorporation, (iv) registered office and representative/service address; (v)

members of the administrative body (e.g., directors) and their function and signatory powers; and (vi) incorporation documents (e.g., deed of foundation, articles of association, statutes, etc).

This information, and supporting documentation, is publicly available for a fee, with limited extracts covering some basic information available without a fee.

In relation to most "private-benefit" foundations (those that are not engaged in commercial activities), the obligation to register documents of incorporation is replaced by an obligation to deposit a notification of formation with the Office of Justice. The notification contains the same basic information (listed above) and is required to be certified as accurate by an attorney, professional trustee or a person licensed under the 180a Act (PGR, Art. 552 (20)(1)).

In relation to associations, the obligation to register is limited to "commercial ventures" and those subject to an audit requirement (see Art. 107(1) PGR for a list of such ventures) while "small" cooperative societies (defined in Art. 483 (1) PGR) are exempt from registration altogether. These activities are not considered to be material to the assessment of this criterion.

Criterion 24.4 **-** The founders of a legal person are required to deliver all incorporation/formation documents to the administrative body (PGR, Art. 182 (3)) covering the information listed under c.24.3. There is no explicit requirement for the administrative body to: (i) ensure that these documents are maintained and available within the country; or (ii) maintain any subsequent changes to these documents. There is requirement for "business books" to be held at the company's registered office (PGR, Art. 182a (2), 1046(1) and 1059(1)) which provide an overview of all business transactions. The authorities consider that, in order to obtain an overview of business transactions, it is necessary to have all formation/incorporation documents and all related resolutions on amendments. However, the statutory basis for this position is not considered to be sufficiently clear by the AT.

Public limited companies (except those that have issued bearer shares – see c.24.11) are required to maintain a register of shareholders, recording the name, date of birth, nationality, domicile of shareholders and, in the case of a legal person, legal name and registered office along with the number and categories of shares held (including voting rights) (PGR, Art. 328 (1)). The shareholders' register must be kept at the registered office of the company (PGR, Art. 329a (2)), which is required to be notified to the Commercial Register Division (PGR, Art. 291) and is required to be an address in Liechtenstein (PGR, Art. 232(1)).

In relation to other legal persons:

Limited liability companies and Anstalten (*establishments)* issuing shares are required to hold a register of members at the registered office, unless the members are entered in the Commercial Register (PGR, Art. 394(3), 402(1) and (2) and 540(6)), in which case the requirement for the company or establishment to maintain a register falls away. This exemption is not in line with the Standard.

Cooperative societies and *trust enterprises* structured in the manner of a corporation are not required to maintain a register of members but are instead required to submit a list of members to the Commercial Register Division at registration and when there are subsequent changes (PGR, Art. 432(3), Art. 433(3) and Art. 468(1)). The list at the Commercial Register Division shall be open to public inspection.

European Companies and *partnerships limited by shares* are subject to the same requirements as public limited companies, as described above (SE-VO, Art. 15 and PGR, Art. 368(3)).

European Cooperative Societies are subject to the same requirements as cooperative societies, as described above (SCE-VO, Art. 17).

Criterion 24.5 - Prior to registration of a legal person, the Commercial Register Division reviews the documents presented and must be satisfied that the requirements for registration are met (PGR, Art. 986). The same applies to applications for changes to information entered in the Commercial Register which must be communicated to the Commercial Register Division, along with supporting documents (PGR, Art. 965(1) and Art. 120).

Information set out in c.24.3 - Art. 965 of the PGR states that "registration for entry of the changes must be filed without delay". The term "without delay" is not defined in the law, but legal materials on which the provision is based state that it means "as soon as possible" after the resolution of the change, which does not ensure that this is done on a "timely basis". Also, where an obligation to notify a change is not fulfilled, the Commercial Register Division must first request that the required change or deletion be notified within 14 days (PGR, Art. 968 (1)) which may have the effect of further delaying the update. However, it should be noted that changes to the information listed under c.24.3 (except for non-registered foundations) have no legal effect with respect to third parties until registered in the Commercial Register and so it is in the interest of parties concerned to register the change. Prior to registration, changes take effect only in the internal relationship of the legal person (PGR, Art. 950(2) and (3)). On this basis, whatever is entered into the Commercial Register is, as a matter of law, always accurate and up to date, though it is possible that false information may be given to the registrar or that there is a delay in reporting changes.

The Commercial Register Division is empowered to request the records of legal persons, in order to ensure that obligations to register changes have been complied with (PGR, Art. 967(3) and 968 (2)). This power is also available to examine whether an entry in the commercial register is in accordance with the facts (PGR, Art. 968(1)).

Similarly, non-registered foundations must notify any changes to information previously notified within 30 days and these must be certified in writing by an attorney, professional trustee or a person licensed under the 180a Act (PGR, Art. 552 (20)(3)). STIFA is empowered to inspect non-registered foundations to ensure that information in the commercial register corresponds to the information held at the foundation (e.g., statutes of the foundation) (PGR, Art. 552 § 21).

Information on shareholders set out under c.24.4 - A change in the legal ownership of a company or similar legal person that issues registered shares does not have effect until such time as that change is entered into the share register (PGR, Art. 328(2)) and so a person that acquires shares cannot vote or receive dividends prior to the transfer of shares being recorded in the register of shares. The same applies also to bearer shares, where the person entered into the register held by the custodian (see c.24.11) shall be considered the shareholder (PGA, Art. 326c(2)). On this basis, whatever is entered into the share register (legal ownership) is, as a matter of law, always up to date and accurate (see above).

For legal persons that are predominately non-trading and wealth management structures (around 80% of legal persons) and required to appoint a qualified member to the governing body, that person is responsible for monitoring transactions performed in the course of the business relationship, in a timely manner, at a level that is commensurate with risk, to ensure they are consistent with business profile (DDA, Art. 9(1)). It has been explained that the qualified member is expected to verify that dividend payments are made to those persons who are registered as shareholders in the share register (for both bearer and registered shares). No similar mechanism is in place to ensure that changes are registered for other legal persons (around 20%), except for bearer shares where the custodian is subject to an audit/review– see c.24.11.

All competent authorities are empowered to inspect registers of registered and bearer shares (PGR, Art. 329(b)(2) (registered shares) and Art. 326d(2) (bearer shares) - within the scope of their competences - to ensure that these registers are properly maintained and kept.

Criterion 24.6 - Liechtenstein utilises three mechanisms to ensure access to information on the BO of a legal person: (i) a central register of BO which is maintained by the Office of Justice; (ii) a requirement for most legal persons to have a qualified member; and (iii) use of share registers (in particular, for those companies with commercial operations in Liechtenstein where there is no use of nominee shareholders). In addition, BO information is generally available through persons subject to the DDA.

The central register was established in 2019 to cover BO for most legal persons. This was extended to also cover BO of partnerships by the Law on the Register of BO of Legal Entities on 1 April 2021. The Law on the Register of BO of Legal Entities applies to all group A legal persons (see c.24.1), but not to auxiliary funds, unregistered partnerships, communities of property, consortia silent partnerships, homesteads and entailed estates and simple communities of rights (which are not considered to be material for the purposes of R.24). It should also be noted that two significant elements have only recently been introduced, with a "transition period" for compliance by 1 October 2021, namely: (i) the obligation for partnerships to enter their BO information on the central register; and (ii) the extension of the definition of BO of a foundation (or trust) to include a founder/settlor who does not exercise control. The number of partnerships is small (around 50 as of 31 December 2020).

Legal persons are required to (i) establish and verify the identity of their BOs (Law on the Register of BO of Legal Entities, Art. 3(1) and (2)); and (ii) to communicate this BO information to the Office of Justice within 30 days of their entry into the Commercial Register or submission of notice of formation (in case of non-registered foundations) (Law on the Register of BO of Legal Entities, Art. 4). There is also a requirement for BOs to provide all necessary information to the legal person (Law on the Register of BO of Legal Entities, Art. 5).

For these purposes, the definition of BO corresponds to the definition in the DDA/DDO. In the case of companies, the BO is the natural person who ultimately directly or indirectly holds 25% or more of the shares or otherwise exercises control over the legal person (VwbPV, Art. 2 (1) (a)). In the case of legal persons holding shares or nominee shareholders, the natural person(s) ultimately holding the shares or controlling the legal person is the BO and has to be entered into the BO register.

There is no specific power available to a legal person that believes that a BO has not provided all necessary information, nor any direct sanction applicable to a BO who does not provide such information. However, all legal persons (except partnerships) are required to have a qualified member on their governing body who is a professional trustee, except those subject to the Business Act or another specialised law (Art. 180a, PGR). A qualified member has to be a professional trustee licensed under the Trustees Act or a person licensed under the 180a Act, who will be supervised by the FMA and subject to the obligations of the DDA/DDO requiring, inter alia, identification and verification of the BO of the legal person. A qualified member is required to terminate its business relationship with a legal person when it is unable to properly identify the legal person's BOs (DDA, Art. 5(3)). BO information must be held by that qualified member at a storage site in Liechtenstein that is accessible at all times, though that location does not need to be specified.

Criterion 24.7 – Legal persons subject to the Law on the Register of BO of Legal Entities (see c.24.6) are subject to an ongoing obligation to establish and verify the identity of the BO and, where there are doubts about information already held, to repeat this process (Law on the Register of BO of Legal Entities, Art. 3(1) to (3)). All legal persons are required to notify the Office of Justice of any changes concerning BO information previously submitted. These must be reported within 30 days of knowledge of the change (Law on the Register of BO of Legal Entities, Art. 4(5)).

Upon receipt of a submission, the Office of Justice is required to verify that the information is complete and perform random checks on the plausibility of the information submitted with access to all information necessary for the inspection (Law on the Register of BO of Legal Entities, Art. 23(2)(a) and (b) and 24(6))). It should be noted that the power to conduct random checks on the plausibility of data is a recent one, and checks are planned from 1 October 2021.

If there is reason to assume that a legal person has violated provisions of the Law on the Register of BO of Legal Entities, an inspection may be carried out by the Office of Justice (Law on the Register of BO of Legal Entities, Art. 23 and 24).

With regard to BO information held by qualified members, they are subject to a requirement to ensure that documents, data or information collected is kept up to date (in line with risk) (DDA, Art. 8(2)) and must repeat due diligence if, during the course of a business relationship, doubts arise concerning the identity of the BO (DDA, Art. 7(3)).

Criterion 24.8 – There is no requirement to have a specific contact or representative accountable to competent authorities for notifying or submitting all relevant basic and BO information. Rather all members of a legal person's administrative body are responsible for the legal person's obligations. Whilst it is possible that members of the administrative body may be based outside Liechtenstein, the qualified member of the administrative body (where there is one) must have a place of business in Liechtenstein (Trustees Act, Art. 3(1)(e) and 180a Act, Art. 14(1)(c) and 4 (1) (d)).

Legal persons are required to appoint a legal representative who must be domiciled in Liechtenstein (unless a domestic address for service has been designated) but this person, while acting as a contact for notifications, etc. is not required to be responsible for the provision of basic or BO information.

As set out at c.24.6 and c.24.7 above, each qualified member must obtain BO information, in accordance with the provisions of the DDA/DDO. As a supervised person, the qualified member must provide such information to the supervisory and other authorities on request (DDA, Art. 19a and 31(1)(a) and CPC, Art. 96b). Whilst the qualified member is not legally responsible for providing BO information on behalf of the legal person to the authorities, when requested to do, they will be under an obligation to comply with such request. This mechanism applies to around 80% of all legal persons but not to those companies with commercial operations in Liechtenstein.

Criterion 24.9 - The Commercial Register Division is obliged to maintain all information registered for 30 years after dissolution of a legal person (Commercial Register Ordinance, Art. 20 (1)). The Office of Justice is required to maintain data held on the BO register for five years after the deletion of a legal person from the Commercial Register (Law on the Register of BO of Legal Entities, Art. 12 (5) (a)).

In addition, legal persons are themselves required to maintain "accounting records" (PGR, Art. 1045 and 1059). "Business books" (the latter arguably covering the information listed under c.24.4 and register of bearer shares) of a dissolved company (or other entity with legal personality) must be retained by the liquidator (or insolvency administrator) for ten years after the legal person ceases to exist (PGR, Art. 142(1)). Similar provisions apply to partnerships (PGR, Art. 728 and 733). The Law on the Register of BO of Legal Entities does not include a requirement for legal persons to maintain BO information post dissolution.

For those legal persons with a qualified member, the record keeping requirements for these professionals under the DDA/DDO apply for ten years from the end of the business relationship (DDA, Art. 20 (1)).

Criterion 24.10 – Qualified members, along with other FIs and DNFBPs, are subject to the full range of supervisory and investigative powers available to competent authorities (CPC, Art. 92, 96(2) and 96b and DDA, Art. 19a(1) and 28(4)).

In relation to legal persons, access to such information is available to law enforcement authorities by way of a court order. This is either executed by a search warrant (CPC, Art. 92) or a request of a judge (CPC, Art. 96(2)). It should be noted that criminal proceedings (investigations) must be initiated in order to apply for a court order, although the level of proof/threshold for initiating investigations for ML and/or associated predicate offences is "simple suspicion". An application can be made immediately to the court within the framework of a preliminary investigation and the order made by the court usually provides for a period of 14 days for the information to be submitted. If necessary, however, this period can be shortened to a few days in urgent cases.

All information on the Commercial Register can be directly accessed by the FIU, FMA, Chamber of Lawyers, National Police, OPP, Court of Justice, and Fiscal Authority (PGR, Art. 955b(2)). This access also applies to dissolved legal persons (30 years – see c.24.9 above). In individual cases, the same authorities may, without limitation, access data on BO held by the Office of Justice (Law on the Register of BO of Legal Entities, Art. 13 and 14) as far as is necessary for AML/CFT purposes and fighting ML predicate offences. It must be ensured that the legal persons concerned are not warned of the retrieval of data.

In addition, all domestic authorities and courts may inspect the share register and register of bearer shares held by the custodian and make copies within the scope of their competence (PGR, Art. 329b(2) and 326d(2)).

Criterion 24.11 - Bearer shares may be issued by public limited companies, partnerships limited by shares and European Companies (PGR, Art. 323 and Art. 368 (3), and SEG, Art. 2). In such cases, they must appoint a custodian and deposit all bearer shares with that custodian, except where they are listed companies that are subject to stock exchange rules or certain types of investment funds (which are directly subject to the DDA but may not have identified the BO of investors in line with the exemption in Art. 22b of the DDO) (PGR, Art. 326a). Bearer shares issued prior to entry into effect of these immobilisation rules (1 March 2013) had to be deposited with a custodian for registration by 1 March 2014, otherwise voting rights would be excluded and dividend payments held in escrow. Since that deadline, bearer shares issued prior to entry into effect of immobilisation rules can be deposited with the custodian for registration only if the shareholder concerned submits a ruling of the Court of Justice that they are the lawful owner of the bearer shares. Bearer shares not registered by 1 March 2024 must be declared void by the company, so that no rights may be asserted on the basis of such shares after that date. This transitional period enables shareholders previously unaware of their status to still pursue their rights. There are no known cases in which bearer shares have not yet been deposited with a custodian.

A custodian must be either: (i) subject to regulation and supervision under the DDA, or regulation and supervision abroad equivalent to the EU AMLD; or (ii) have a registered office in Liechtenstein and a bank account in the shareholders' name in Liechtenstein or an EEA member state (PGR, Art. 326b(1) and (2)). However, these requirements do not apply to legal persons specified in Art. 180a(3) PGR i.e., legal persons which, pursuant to the Business Act or another specialised law (e.g., Banking Act, Trustees Act, and Asset Management Act) are required to have a general manager or which are supervised by the Government, a municipality, the land transfer authority, or another authority (PGR, Art. 326b(3)) (domestic operating companies). In these cases, the custodian need not be regulated or supervised or have a registered office in Liechtenstein. Rather, a bank account in Liechtenstein or another EEA member state in the name of the shareholder is sufficient. The custodian is subject to an annual audit/review with regard to compliance with their duties (PGR, Art. 326i). In the course of the audit/review it is verified that:

(i) the person receiving dividends is registered in the share register; and (ii) that all information on the shareholder (name, date of birth, domicile, etc.) is entered.

Regardless of the domicile/residence of the custodian in each of the above cases, the register of bearer shareholders must in all cases be kept by the custodian at the registered office of the legal person (PGR, Art. 326c(5)), ensuring that the register is in Liechtenstein. Inter alia, the following must be entered in the register for each bearer shareholder: (i) surname and first name; (ii) date of birth; (iii) nationality and domicile; and (iv) in the case of a legal person, legal name and registered office (PGR, Art. 326c(1)). The person entered in the register shall be considered the shareholder (PGR, Art. 326c(2)).

The above provisions do not expressly deal with bearer share warrants (as defined in the FATF Recommendations) and there is no express prohibition in the PGR on the use of such warrants.

The provisions of the Law on the Register of BO of Legal Entities applies also to those legal persons that can issue bearer shares. Accordingly, BO information must be entered in the BO register and is accessible via this register.

Criterion 24.12 - There is no prohibition against the use of nominee shareholders or nominee directors by legal persons.

There is no requirement for nominee shareholders or nominee directors to disclose the identity of their nominator to the legal person, Commercial Register, or to the Office of Justice. The obligation to identify BOs and report the same to the relevant register attaches itself to the legal person (see c.24.6) and does not extend to disclosure of all nominators. Whilst BOs are required to provide the legal person with all information necessary for fulfilling its duties (Law on the Register of BO of Legal Entities, Art. 5), this may be interpreted as a requirement only to provide information when requested to do so and the requirement cannot be directly enforced (see c.24.6). Registers of shareholders or members kept by the legal person are not required to disclose the identity of nominators of nominee shareholders or directors.

Persons providing nominee services (as shareholders or directors) on a professional basis are required to be licensed by the FMA or (up to 31 December 2025) the Office of Economics and are subject to the DDA. Whilst nominee shareholders or directors that are not acting by way of business (i.e., without the possibility of making a profit) are not regulated, the threshold for acting on a "professional basis" is set very low (Liechtenstein Supreme Court decision of 1 April 2011, 03 ES.2010.15[49]) and the authorities consider that such activities are very rarely performed. Moreover, there is no requirement that legal persons only use nominees that are licenced in Liechtenstein. The effect of this is that unlicensed and foreign nominees may be used by legal persons and whilst third parties are able to compare publicly available information on board members (Commercial Register) to information published by the FMA on professional trustees and persons registered under the 180a Law (acting in a nominee capacity), this will not highlight nominee directors acting other than by way of business, or which are regulated and supervised outside Liechtenstein.

Nominee directors and nominee shareholders that are subject to the obligations of the DDA are obliged to identify and verify their nominator as a BO of the legal person and to make this information available to the competent authorities upon request (see c.24.10). Registers of shareholders or members are not required to disclose the nominee status of licenced nominees.

[49] The decision states: if the transactions corresponding to the founding activities are concluded in a manner that leaves open the possibility of making a profit, the profit-making intention does already exist. Even the intention of achieving a merely indirect economic advantage is sufficient. Whether a profit is actually made is irrelevant. …".

To the extent that a nominator is also a BO, then the requirement for most legal persons to have a qualified member (see c.24.6) who is responsible for identifying and verifying the identity of the BO (as part of CDD measures), will ensure that nominees are not misused.

Criterion 24.13 – The fine for failing to file basic information is up to CHF 5 000 in the case of deliberate omission or up to CHF 1 000 for a negligent omission. These fines rise to CHF 10 000 in the case of non-registered foundations (PGR, Art. 977(1)(1)) and SchlTPGR, Art. 65(3) and (4) and Art. 66c). Higher fines apply where information filed is incorrect. The fine may be imposed repeatedly until the application has been submitted or registration has been carried out (SchlTPGR, Art. 65(4) and 66c(2)). However, penalties for not updating information (PGR, Art. 967 and 968) are only applicable following a request to do so being issued by the Office of Justice and no penalty is directly applicable to a breach of PGR, Art. 965 (requirement to file changes without delay). In addition, a legal person may be dissolved or liquidated by the Commercial Register Division (PGR, Art. 130 et seq and Art. 971) following a grace period of two months which is allowed to restore a lawful state of affairs.

The Court of Justice may impose a fine of up to CHF 10 000 on anyone who deliberately violates his duties for the proper keeping of a register of shareholders (SchlTPGR, Art. 66e). If the person acts negligently, the fine is CHF 5 000. This fine may be imposed repeatedly until the lawful state of affairs is restored (SchlTPGR, Art. 66e(2)).

A breach of the obligation to enter or update BO information in the central BO register may be subject to an administrative fine of up to CHF 200 000 (Law on the Register of BO of Legal Entities, Art. 31(2)(a)). In addition, the Office of Justice may order the liquidation of a non-compliant entity that fails to submit required BO information (Law on the Register of BO of Legal Entities, Art. 23(3)(h)).

A custodian who does not comply with its duties in relation to bearer shares may be subject to a fine of up to CHF 10 000 for deliberate conduct (SchlTPGR, para. 66d)) or up to CHF 5 000 if the custodian acts negligently (SchlTPGR, Art. 66d(3)). The fine may be imposed repeatedly until the custodian complies with its duties (SchlTPGR, Art. 66d(2)).

If no custodian has been appointed or entered in the commercial register, the Commercial Register Division will request the company concerned to fulfil its obligation within 14 days (PGR, Art. 968 (1)). If the company still fails to comply with its obligation, the Commercial Register Division may impose a fine (PGR, Art. 977(1) and SchlTPGR, Art. 65(3) and (4)). See above.

An administrative fine of up to CHF 5 000 may be imposed on a legal person for failing to keep business books (SchlTPGR, Art. 66(1)) and may be imposed on a recurring basis until the obligation has been fulfilled (PGR, Art. 66(3)).

This range of sanctions outlined above can be applied proportionately to greater or lesser breaches of requirements.

Criterion 24.14 – The Liechtenstein legal framework allows authorities to provide international cooperation in relation to basic and BO information through various channels:

(a) Basic information maintained by the Commercial Register for all legal persons is available publicly and/or may be requested and obtained by any person, including foreign competent authorities.

(b) Information on BO held by the Office of Justice can be accessed in individual cases by competent authorities (including the FIU, the FMA, the National Police, the OPP and the Chamber of Lawyers) who may also transfer this data to requesting foreign authorities (Law on the Register of BO of Legal Entities, Art. 13 and 14).

(c) All investigative powers of law enforcement authorities are applicable in MLA proceedings (MLA Act, Art. 9(1)). The average execution time for MLA requests was 59 calendar days in 2020 which cannot be considered "rapid". However, it is not possible to evaluate only MLA requests concerning BO data, as MLA requests are regularly not limited to BO information.

The FIU has a power to pass official information that is not accessible to the public to foreign FIUs (FIU Act, Art. 7(2)), though it is not explicitly given the responsibility to do so (FIU Act, Art. 4 and 5). The average response time to requests from foreign counterparts of the FIU is 10 to 15 working days which is well within the turnaround time of one month set by the Egmont Group for responses to be provided to incoming requests for information (though, arguable, this cannot be considered "rapid").

Supervisory authorities may request all information (including BO information) from FIs and DNFBPs that they require to perform their functions under the DDA, including co-operation with foreign supervisory authorities (DDA, Art. 28(4) and 37).

Criterion 24.15 - The FMA maintains a register of all outgoing requests (including time taken by foreign authorities to respond to the request) and monitors the quality of assistance upon receipt of the information.

The Chamber of Lawyers has, to date, neither made nor received any requests for assistance.

The Office of Justice maintains a register of incoming and outgoing requests regarding mutual legal assistance. While the quality of assistance received is not formally monitored by the Office of Justice or Court of Justice, anecdotal indications are that there are no issues in obtaining BO information via mutual legal assistance, although, in some cases, mutual legal assistance may take some time to complete, regardless of the country in question. Basic and BO information is requested in around 95% of MLA requests to foreign countries. In particular, knowledge of BO is central to investigating ML or predicate offences to ML (analogously in the case of TF), in order to identify all persons involved and thus the possible perpetrators.

Weighting and Conclusion

Two criteria have been rated partly met: (i) requirement placed on companies to hold basic information in Liechtenstein (c.24.4); and (ii) nominee arrangements (c.24.12). None of the shortcomings identified under these two criteria are considered to impair access to adequate, accurate and up-to-date information on the BO and control of legal persons and so **R.24 is rated LC.**

Recommendation 25 – Transparency and beneficial ownership of legal arrangements

Liechtenstein was assessed as LC for R.34 in the 2014 MER. The report noted issues in relation to the FMA's access to BO information and concerns over the effectiveness of trustee supervision impacting the adequacy and accuracy of information on BO held by trustees.

For the purposes of this Recommendation, Liechtenstein authorities confirm that there are no other legal arrangements comparable to trusts contemplated by Liechtenstein law.

Criterion 25.1 - (a) The following legal provisions address this requirement:

All trusts governed under Liechtenstein law[50], including those without a Liechtenstein trustee, are required to: (i) establish and verify the identity of their BOs (Law on the Register of BO of Legal Entities, Art. 3(1) and (2)); and (ii) to communicate this BO information to the Office of Justice within a prescribed timeframe[51]. In practice this obligation applies to "members of the managerial level and other natural persons" who acted or should have acted for the trust (Law on the Register of BO of Legal Entities, Art. 32), which is taken to refer to the trustee (if an individual) or members of the governing body (if the trustee is a legal person). However, this is not clearly stated[52]. In some cases, communication may take up to one year and 30 days as the requirement to provide BO information is linked to entry in the Commercial Register or submission of trust deed to the Office of Justice[53] (Law on the Register of BO of Legal Entities, Art. 4(4) and PGR, Art. 900 and 902). The BO definition in Art. 2(1)(a) of the Law on the Register of BO of Legal Entities and Art. 2(1)(b) of the VwbPV corresponds with the BO definition of the DDA/DDO, so includes the settlor(s), the trustee(s), the protector(s)(if any), the beneficiaries or class of beneficiaries, and any other natural person(s)exercising ultimate effective control over the trust. Whilst there is no direct obligation to hold information that is established and verified, the trust (through the trustee) must do so in order to be able to grant to the Office of Justice unrestricted access to all information that is relevant in connection with the fulfilment of the trust's duties under the Law on the Register of BO of Legal Entities (Law on the Register of BO of Legal Entities, Art. 24(6)).

In addition, professional trustees in Liechtenstein are subject to the DDA/DDO, and so are required to identify and take reasonable measures to verify, on a risk sensitive basis, the identity of the BO, which, in the case of trusts includes the settlor(s), the trustee(s), the protector(s) (if any), the beneficiaries (or class of beneficiaries) and any other natural person(s) exercising ultimate effective control over the trust (DDO, Art. 3). There is long-standing case law which sets the threshold for what is to be understood as "professional basis" at a very low level (Liechtenstein Supreme Court decision of 1 April 2011, 03 ES.2010.15)[54]. They must also hold this information (DDA, Art. 20(1)).

Trusts with non-professional trustees (which are not subject to the DDA/DDO) account for 6% of trusts in Liechtenstein and are set up by Liechtenstein citizens to manage family assets where family members act as trustee.

In a case where the Law on the Register of BO of Legal Entities does not apply (trust administered by TCSP supervised by the FMA where BO information for the trust has been registered in a BO

---

[50] Except trusts administered by TCSPs supervised by the FMA where BO information for the trust has been registered in a BO register of another EEA Member State (Law on the Register of BO of Legal Entities. Art. 2(1)(c)).

[51] For trusts already in existence on 1 April 2021, a transitional provision gives six months in which to provide information on any settlor who does not exercise control to the Office of Justice (a requirement additional to that in force prior to 1 April 2021).

[52] Where violations are committed by a trust, the penal provisions shall apply to the trustee (Law on the Register of BO of Legal Entities, Art. 32).

[53] Every trust created for a period of more than twelve months shall within twelve months from its establishment be registered for entry in the Commercial Register if the trustee or at least one of several co-trustees is resident or domiciled in Liechtenstein (PGR, Art. 900(1)). There is no obligation to enter a trust in the Commercial Register where an original or certified copy of the deed of formation is deposited with the Office of Justice within twelve months (PGR, Art. 902).

[54] The decision states: if the transactions corresponding to the founding activities are concluded in a manner that leaves open the possibility of making a profit, the profit-making intention does already exist. Even the intention of achieving a merely indirect economic advantage is sufficient. Whether a profit is actually made is irrelevant. …".

register of another EEA Member State), then that TCSP, like all professional trustees in Liechtenstein, will be subject to the DDA meaning that all trustees of express trusts governed by Liechtenstein law are required to obtain BO information.

(b) Trustees are required to keep a *schedule of assets* concerning the trust property in accordance with the provision of Art. 1045(3) PGR, updated annually, and maintain records and vouchers for at least ten years (PGR, Art. 923(1) in conjunction with Art. 1059). The concept of "business books" in Art. 1059 extends to information on relationships with other regulated agents of, and service providers to, the trust.

(c) Professional trustees are subject to the DDA, and therefore required to keep information and documents for ten years from the end of the business relationship with a trust (DDA, Art. 20 (1)). Furthermore, the trustee is obliged to maintain records and vouchers for at least ten years (PGR, Art. 923(1) in conjunction with Art. 1059).

Criterion 25.2 – All trusts governed under Liechtenstein law[55] are subject to an ongoing obligation (through the trustee – see c.25.1) to establish and verify the identity of the BO and, where there are doubts about information already held, to repeat this process (Law on the Register of BO of Legal Entities, Art. 3(1) to (3)). Trusts (through the trustee) are required also to update information submitted to the Office of Justice within 30 days of becoming aware of any changes (see R.24). As noted above, in some cases, the authorities may not be made aware of the existence of a trust for up to one year and 30 days after settlement (Law on the Register of BO of Legal Entities, Art. 4(4) and PGR, Art. 900 and 902) and so the obligation to inform the Office of Justice of a change will not apply.

In addition, professional trustees subject to the DDA are subject to an ongoing requirement to establish the identity of the BO of a trust and are required to keep information and documents already held up to date (DDA, Art. 5).

Criterion 25.3 - Trustees are required to disclose their status to persons subject to the DDA (i.e., FIs and DNFBPs) (Law on the Register of BO of Legal Entities, Art. 4 (6)) at the time of establishing a business relationship or carrying out an occasional transaction.

Criterion 25.4 **–** There are no legal provisions or restraints that would prevent trustees from providing competent authorities with any information. The authorities' powers to obtain such information has not been subject to any legal challenge. In the case of sharing information with FIs and DNFBPs, the trustee is required to promptly provide BO data when disclosing their status (Law on the Register of BO of Legal Entities, Art. 4(6)). This provision does not deal with information on assets or where there is a subsequent change in BO or information held. In such a case, so long as the trustee has entered into a trust administration agreement with its client, in which the trustee's duties in the context of the administration of the trust are specified, then this transfer of data will be possible under Art. 6 (1)(b) of the GDPR.

Criterion 25.5 **–** Professional trustees, along with other FIs and DNFBPs, are subject to the full range of supervisory and investigative powers available to competent authorities (CPC, Art. 92, 96(2) and 96b; DDA, Art. 28(4); and FIU Act, Art. 5a in conjunction with DDA, Art. 19a). This includes access to all relevant information held by the trustee, FI or DNFBP.

In relation to non-professional trustees, access to such information is available to law enforcement authorities by way of a court order. This is either executed by a search warrant (CPC, Art. 92) or a request of a judge (CPC, Art. 96(2)). It should be noted that criminal proceedings

[55] Except trusts administered by TCSPs supervised by the FMA where BO information for the trust has been registered in a BO register of another EEA Member State (Law on the Register of BO of Legal Entities Art. 2(1)(c)).

(investigations) must be initiated in order to apply for a court order, although the level of proof/threshold for initiating investigations for ML and/or associated predicate offences is "simple suspicion". An application can be made immediately to the court within the framework of a preliminary investigation and the order made by the court usually provides for a period of 14 days for the information to be submitted. If necessary, however, this period can be shortened to a few days in urgent cases.

All information on the Commercial Register can be directly accessed by the FIU, FMA, Chamber of Lawyers, National Police, OPP, Court of Justice, and Fiscal Authority (PGR, Art. 955b(2)). In individual cases, the same authorities may, without limitation, access data on BO held by the Office of Justice (Law on the Register of BO of Legal Entities, Art. 13 and 14) as far as is necessary for AML/CFT and fighting ML predicate offences. It must be ensured that the trusts concerned are not warned of the retrieval of data.

Criterion 25.6 **–** The Liechtenstein legal framework allows authorities to provide international cooperation relating to information on trusts.

(a) In relation to registered trusts, all the information collected by the Commercial Register Division is publicly available and anyone (including foreign competent authorities) is entitled to access information and supporting documents. This covers: (i) designation of the trust; (ii) date of formation of the trust; (iii) duration of the trust; and (iv) last name, first name, and place or residence or legal name and domicile of the trustee.

(b) Information on BO held by the Office of Justice can be accessed in individual cases by competent authorities (including the FIU, the FMA, the National Police, the OPP and the Chamber of Lawyers) who may also transfer this data to requesting foreign authorities (Law on the Register of BO of Legal Entities, Art. 13 and 14).

(c) All investigative powers of law enforcement authorities are applicable in MLA proceedings (MLA Act, Art. 9 (1)). The average exercise execution time for MLA requests was 59 calendar days in 2020 which cannot be considered "rapid". However, it is not possible to evaluate only MLA requests concerning BO data, as MLA requests are regularly not limited to BO information.

The FIU has a power to pass official information that is not accessible to the public to foreign FIUs (FIU Act, Art. 7(2)), though it is not explicitly given the responsibility to do so (FIU Act, Art. 4 and 5). The average response time to requests from foreign counterparts of the FIU is 10 to 15 working days which is well within the turnaround time of one month set by the Egmont Group for responses to be provided to incoming requests for information (though, arguably, this cannot be considered "rapid").

Supervisory authorities may request all information (including BO information) from persons subject to the DDA that they require to perform their oversight functions. This specifically includes information to facilitate co-operation with foreign counterparts (DDA, Art. 37).

Criterion 25.7 - Professional trustees are subject to the sanctions established by the DDA, in relation to obligations under that Act (see R.27), and to the sanctions that can be imposed by the Office of Justice in relation to obligations concerning the Commercial Register and central BO register (the latter by virtue of Art. 32 of the Law on the Register of BO of Legal Entities which applies penal provisions to the trustee or other natural person who acted or should have acted on behalf of the trust). See c.24.13 above. These are proportionate and dissuasive.

Non-professional trustees are not subject to the DDA, but they are subject to sanctions under the PGR and Law on the Register of BO of Legal Entities (the latter by virtue of Art. 32 of the Law on the Register of BO of Legal Entities which applies penal provisions to the trustee or other natural person who acted or should have acted on behalf of the trust).

Failure to comply with obligations to establish and verify BO and to communicate this to the Office of Justice are subject to an administrative fine of up to CHF 200 000 (VwbPG, Art. 31(2)). The Office of Justice can also order the "liquidation" of a trust in the event of failure to communicate required BO data (VwbPG, Art. 23(3)(h)).

Criterion 25.8 - There is a range of civil and criminal sanctions available to deal with failure to grant authorities timely access to information regarding trusts.

Refusal to surrender documents under a search warrant or court order may bring a fine of up to CHF 10 000 and, if the refusal continues, imprisonment for up to six weeks (CPC, Art. 96(2)).

The Court of Justice may impose a fine of up to CHF 100 000 on any person who fails to provide to the FIU the information referred to in Art. 19a(1) DDA (information for analytical purposes) or withholds significant facts in this connection (DDA, Art. 30(2a)). This power is used to obtain information regarding trusts.

Professional trustees are subject to Art. 31 (1) (a) DDA, pursuant to which a supervisory authority may impose a fine of up to CHF 200 000 on any person who wilfully refuses to give information when requested.

Weighting and Conclusion

There are only minor shortcomings, including placing obligations under the Law on the Register of BO of Legal Entities on trusts rather than the trustee.

R.25 is rated LC.

Recommendation 26 – Regulation and supervision of financial institutions

Liechtenstein was assessed as LC for R.23 in the 2014 MER. The report noted several issues in relation to effectiveness, including the use of audit firms to conduct inspections and the absence of a clear risk-based approach to supervision.

The introduction to R.10 lists activities to which the DDA does not apply and so which are not subject to regulation and supervision.

Whereas for prudential purposes, the FMA regulates and supervises managers of investment funds, the DDA applies not to these managers (except in the case of individual portfolio management provided by fund management companies) but to the underlying funds that they manage. Information has not been provided by the authorities on the application of market entry requirements to investment funds, where persons other than those authorised in respect of the manager may hold management functions in the case of corporate funds.

Criterion 26.1– Responsibility for oversight of covered FIs' compliance with the AML/CFT framework resides with the FMA (DDA Art. 23(1)(a)). This includes EEA FIs and Swiss insurance undertakings and intermediaries that operate through an "establishment" in Liechtenstein, which covers branches, agents, and representative offices. It does not include EEA FIs or Swiss insurance undertaking and intermediaries operating with the scope of freedom to provide services.

The FMA is the supervisory authority in relation to all covered FIs, as well as VASPs and all DNFBPs (except lawyers and law firms, which are supervised by the Chamber of Lawyers).

The introduction to R.10 lists activities to which the DDA does not apply and so which are not subject to regulation and supervision.

Criterion 26.2 – With one exception, covered FIs that operate in, or from, Liechtenstein require a licence from the FMA to take up business (AIFMG, Art. 28(1) to (3); Asset Management Act, Art. 5; Banking Act, Art. 15, 30s, 30t, 30u and 30v; E-Money Act, Art. 4; Insurance Supervision Act, Art.

11; Insurance Distribution Act, Art. 5; Investment Undertakings Act, Art. 22(1); Payment Services Act, Art. 7; Post Organisation Act, Art. 14 and 15; and UCITS Act, Art. 13. Conducting an activity without a licence constitutes a misdemeanour and is punishable by the Court of Justice. The only exception is exchange bureaux, which are required to be registered with the Office of Economic Affairs.

No licence is required in Liechtenstein for: (i) EEA FIs that operate through an establishment in Liechtenstein or which operate within the scope of freedom to provide services where licensed in the EEA by a responsible supervisory authority; or (ii) Swiss insurance undertakings and intermediaries, that operate through an establishment in Liechtenstein or which operate within the scope of freedom to provide services where licensed in Switzerland, as stipulated in the Direct Insurance and Insurance Distribution Agreement between Switzerland and Liechtenstein (Art. 10 et seq of the annex; and Art. 32 et seq of the annex). However, home competent authorities must notify the FMA in advance in the case of such operations and notification procedure in place - as detailed by the ESAs - provides for a supervisory exchange on the FI's business case and risk profile, which permits the FMA as host supervisor to raise any concerns it may have with the notifying home supervisor.

All covered FIs are supervised by the FMA (FMA Act, Art. 5) and are subject to supervision for AML/CFT purposes (DDA, Art. 3(1)).

The operation of a domiciliary bank (shell bank) is prohibited. Domiciliary banks are banks that do not maintain a physical presence in the country of incorporation and that are not part of a group operating in the financial sector that is subject to appropriate consolidated supervision and governed by Directive 2005/60/EC or equivalent regulation (Banking Act, Art. 15 (4)).

Criterion 26.3 - Measures to prevent criminals or their associates from holding, or being the BO of, a significant controlling interest or holding a management function in a covered FI are set out in sector specific laws.

Any intended direct or indirect acquisition, any intended direct or indirect increase, and any intended sale of a "qualifying holding" must be notified to the FMA (AIFM Act, para. 34 and AIFM Ordinance, Art. 33; Asset Management Act, Art. 10a; Banking Act, Art. 26a; E-Money Act, Art. 9; Insurance Distribution Act, Art. 8(1)(k); Insurance Supervision Act, Art. 92(1); Investment Undertakings Act, Art. 25; Payment Services Act, Art. 17; and UCITS Act, Art. 19).

Pursuant to Art. 6 of the Post Organisation Act, Liechtenstein must always hold at least 51% of the shares of the Post Office in terms of capital and voting rights. These shares are not transferable. Since 2005, Liechtenstein has held 75% of the shares; the remaining 25% are hold by Swiss Post.

The term "qualifying holding" is defined as a direct or indirect holding in another undertaking which represents 10% or more of the voting rights or capital or which makes it possible to exercise a significant influence over its management (AIFM Act, Art. 4(1)(32); Asset Management Act, Art. 4(1)(p); Banking Act, Art. 1(3); E-Money Act, Art. 1(2); Insurance Supervision Act, Art. 10(36); Investment Undertakings Act, Art. 2 (1)(m); Payment Services Act, Art. 17(1); and UCITS Act, Art. 3(1)(13). No definition is included in the Insurance Distribution Act, which instead requires the provision of "information on the identity of shareholders, members or partners, or other rights holders, whether natural or legal persons, who hold more than 10% in the applicant" and those with close links to the applicant (Art. 8). Only natural persons may be the ultimate shareholders.

Persons holding a "qualifying holding" (or equivalent under the Insurance Distribution Act) are required to meet fit and proper requirements pursuant to each sectoral law (AIFMG, Art. 34; AIFMV, Art. 33; Asset Management Act, Art. 10a to 10c; Asset Management Ordinance, Art. 8; Banking Act, Art. 17(5), 26a, 30s(11), 30t(9) and 30v(1)(b); Banking Ordinance, Art. 27a, 55b

(1)(b), 55I (1)(b) and Annex 8; E-Money Act, Art. 7(1)(d) and 9(1); Insurance Distribution Act, Art. 6, 8 and 9; Insurance Supervision Act, Art. 34 and 94; Investment Undertakings Act, Art. 24 and 25; Investment Undertakings Ordinance, Art. 32; Payment Services Act, Art. 9(1)(f) and 17; UCITS, Art. 15(1)(d); and UCITS Ordinance, Art. 23).

Members of the board and management members of a covered FI have to meet fit and proper requirements pursuant to sectoral laws on an ongoing basis (AIFM Act, Art. 30(1) and Art. 33; Asset Management Act, Art. 6(1)(h); Banking Act, Art. 17, 19, and 28 and Banking Ordinance, Art. 29 and 30; E-Money Act, Art. 7; Insurance Distribution Act, Art. 14, 15, 40(2) and 41(1), and Insurance Distribution Ordinance, Art. 6 and seq; Insurance Supervision Act, Art. 33(1) and Insurance Supervision ordinance, Art. 3, 4(2) and 5); Investment Undertakings Act, Art. 28; Payment Services Act, Art. 9; and UCITS Act, Art. 15(1)(b) and Art. 18).

In line with the above requirements, persons who wish to have a "qualifying holding" or hold a management position at a covered FI must inform (subject to notice of refusal)/apply (subject to approval) in writing to the FMA as follows:

Law	Provision(s)	Inform or apply	Ex ante/ex post
AIFMG/AIFMV	AIFM Act, Art. 33(1) with Art. 30(1) AIFM Ordinance, Art. 30	Inform	Ex ante
Asset Management Act/Ordinance	Asset Management Act, Art. 10 Asset Management Ordinance, Art. 4	Apply	Ex ante
Banking Act/Banking Ordinance	Banking Act, Art. 26 in conjunction with Art. 19 (management position) Banking Act, Art. 26a in conjunction with Banking Ordinance, Annex 8 (qualifying holdings)	Apply	Ex ante
E-Money Act	E-Money Act, Art. 7 in conjunction with Art. 6 (management position) E-Money Act, Art. 9 (qualifying holdings)	Apply	Ex ante
Insurance Distribution Act	Insurance Distribution Act, Art. 12 and 13	Apply (in relation to members of the board, management members and persons active in insurance distribution) Inform (in relation to qualifying holdings)	Ex ante
Insurance Supervision Act	Insurance Supervision Act, Art. 19(1)(a) in conjunction with Art. 12(2)(h) and (i), and Art. 92 Insurance Supervision Order, Art. 3	Apply	Ex ante
Investment Undertakings Act/Ordinance	Investment Undertakings Act, Art. 28	Inform	Ex ante
Payment Services Act/Ordinance	Payment Services Act, Art. 9 (management position) Payment Services Act, Art. 17 (qualifying holdings)	Apply	Ex ante

UCITS and Ordinance	UCITS Act, Art. 18 with Art. 15(1)(b) UCITS Ordinance, Art. 21	Inform	Ex ante

In order to ensure that no criminals (or their associates) hold, or are the BO of, a significant controlling interest or hold a management function in a covered FI, the FMA examines fit and proper credentials under the sectoral laws as follows:

Law	Provision(s)
AIFMG/AIFMV	Management - personal integrity and good reputation Qualifying holdings - criminal records, criminal investigations, or proceedings
Asset Management Act/Ordinance	Management – good repute, honesty, and integrity (supported by criminal record extracts and written statements on any pending criminal proceedings) Qualifying holdings – reputation and indications of ML or TF
Banking Act/Ordinance	Management – good reputation (supported by extract from criminal record) Qualifying holdings - criminal records, criminal investigations, or proceedings
E-Money Act	Management – sound and prudent Qualifying holding - criminal records, criminal investigations, or proceedings
Insurance Distribution Act	Management - good repute (including conviction for an offence against the property of another and registration in a criminal register) Qualifying holding – personal integrity (including criminal records, criminal investigations, and proceedings)
Insurance Supervision Act/Ordinance	Management – personal integrity (including conviction for an offence against the property of another, registration in a criminal register and ongoing criminal proceedings) Qualifying holding – personal integrity and indications of ML or TF
Investment Undertakings Act/Ordinance	Management – right and proper and good reputation Qualifying holding - personal integrity (including criminal records, criminal investigations, and proceedings)
Payment Services Act/Ordinance	Management – sound and prudent Qualifying holding - criminal records, criminal investigations, or proceedings
UCITS and Ordinance	Management – personal integrity Qualifying holding - criminal records, criminal investigations, or proceedings

The FMA follows Joint Guidelines on the prudential assessment of acquisition and increases of qualifying holdings in the banking, insurance, and securities sectors issued by EIOPA, EBA and ESMA (2016) – implemented in Liechtenstein through FMA Guidelines 2017/20. These provide for open and ongoing investigations and proceedings against the proposed acquirer and of any person linked to the proposed acquisition (any person who has, or appears to have, a close family or business relationship with the proposed acquirer). Joint Guidelines – issued in 2017 by ESMA and EBA – on assessing the suitability of members of management and key function holders also provide that on-going investigations should be considered when resulting from judicial procedures. The FMA must take these Joint Guidelines into account (FMA Act, Art. 5(5)).

Whilst not all sectoral laws make explicit reference to the prevention of ownership or management by criminals (or associates of criminals), it is considered by the AT that there is a sufficient legal basis for the FMA to do so with the exception of management under the E-Money Act and Payment Services Act where there is reference only to "sound and prudent management". However, in these cases, as for other FIs, FMA Notice 2013/7 requests evidence to be provided to

the FMA on the reputation, honesty, and integrity of management, including criminal records and relevant information on criminal proceedings.

The following legal provisions require any changes in circumstances of persons with qualifying holdings and board and management members to be notified to the FMA (i.e., criminal record changes post approval):

Law	Provision(s)
AIFM Act/Ordinance	AIFM Act, Art. 33 with Art. 31, and AIFM Act, Art. 30 with AIFM Ordinance, Art. 30 AIFM Act, Art. 34 with AIFM Ordinance, Art. 33
Asset Management Act/Ordinance	Asset Management Act, Art. 7a and 10, Asset Management Act, and Asset Management Ordinance, Art. 4 Asset Management Act, Art. 10a – 10c
Banking Act/Banking Ordinance	Banking Act, Art. 26(2)
E-Money Act	E-Money Act, Art. 6(2)
Insurance Distribution Act	Insurance Distribution Act, Art. 12(1)(a) and 13 in conjunction with Art. 8(1) (k), (l) and (m)
Insurance Supervision Act	Insurance Supervision Act, Art. 19(1)(a) in conjunction with Art. 12(2)(h), (i) and (k), and Insurance Supervision Ordinance, Art. 3 to 5
Investment Undertakings Act/Ordinance	Investment Undertakings Act, Art. 28 and 30 to 32 Investment Undertakings Act, Art. 28 and 25
Payment Services Act/Ordinance	Payment Services Act, Art. 9(5)
UCITS and Ordinance	UCITS Act, Art. 18 with Art. 15 and UCITS Ordinance, Art. 21 UCITS Act, Art. 19 with UCTIS Ordinance, Art. 23

Exchange bureaux are subject to "reliability checks" conducted by the Office of Economic Affairs (Business Act, Art. 11(1)(b) in conjunction with Art. 12, Art. 17, and Art 18). See explanation under c.28.4(b). It is not clear what statutory provisions are in place to deal with associates of criminals.

Criterion 26.4 - a) The regulation and supervision of core principles institutions are said by the authorities to be largely in line with the core principles which are relevant to AML/CFT, including the application of consolidated group supervision for AML/CFT purposes (DDA, Art. 16), but this has not been demonstrated to the AT. Groups are required to establish strategies and procedures that apply across the group, in particular for the purpose of AML/CFT.

The last assessment of Basel, IAIS and IOSCO Principles was conducted by the IMF in 2002/2003, with a follow-up assessment of Basel and IOSCO Principles in 2008. Given the significant changes made to Liechtenstein's regulatory framework since then, these assessments are considered too old to be relevant. There have been no more recent assessments or reviews, internal (self-assessments) or external, for the Basel or IOSCO Principles. However, self-assessments have been conducted since 2015 in respect of the following relevant IAIS Principles: 1, 3, 4, 5, 7, 8, 18 and 25. The FMA's self-assessments were reviewed by the IAIS which concluded in its related reports that all of the above ICPs were either largely observed or observed by the FMA.

b) Regulation and supervision do not differentiate between core principles and non-core principles FIs. All covered FIs, including those providing money or value transfer services and money or currency changing services, are subject to the FMA's risk-based approach to supervision.

***Criterion* 26.5** - The FMA applies a risk-based approach to supervision. Supervisory authorities are required to draw up a risk profile for each covered FI (DDA, Art. 23a (2)). The risk profile is compiled by assessing: (i) the nature, size, complexity, and predisposition to risk of the business; (ii) the arrangements for risk-appropriate monitoring as referred to in Art. 9 of the DDA; (iii) the internal risk assessment as referred to in Art. 9a of the DDA (business risk assessment); (iv) the internal organisational arrangements as referred to in Art. 21 and 22 of the DDA; and (v) the results of previous inspections as referred to in Art. 24 and 25 of the DDA.

This supervisory approach is applied also to groups that have a Liechtenstein parent. There is no explicit legislative basis for doing so.

In the case of sectors classified as having a minor or moderate risk in the NRA, sectoral rather than individual risk profiles may be used instead (DDA, Art. 23a(3)).

The frequency and depth of AML/CFT ordinary inspections (but not supervision more generally) must be driven by the risk profile of covered FIs and groups, and also the results of the NRA (DDA, Art. 23a (4)). The authorities have not clearly explained how the diversity and number of FIs is considered when determining frequency and depth of supervision.

The degree of discretion afforded to covered FIs is not specifically considered when assessing the risk profile of subject persons, as it is mainly limited to the investment fund sector, where the application of the exemption that is available (identification and verification of BOs) is subject to a requirement for a comprehensive risk assessment. Here, the intensity and frequency of supervision takes account of the discretion that is allowed to investment funds through the higher risk classification attached to use of the exemption. However, covered FIs have discretion also in the application of EDD.

Criterion 26.6 – Updates of risk profiles are carried out on a regular basis (DDO, Art. 37(9)). In addition, re-evaluation is conducted following extraordinary inspections, the application of "supervisory measures" or sanctions, and following certain regular inspections.

The FMA takes account of examples provided in para. 57 of the EBA Risk-Based Supervision Guidelines to trigger ad hoc reviews. Thus, the FMA takes, in particular, account of the following to conduct ad hoc reviews of risk profiles: (i) major external events that change the nature of risks; (ii) emerging ML/TF risks, which includes new products and services in new markets and opening of new branches and subsidiaries; (iii) findings from offsite and onsite supervision; (iv) changes to, or new information emerging in relation to, owners of qualifying holdings, members of the management board or key function holders, operations or the organisation; and (v) other situations where the FMA has grounds to believe that information on which it had based its risk assessment is no longer relevant or has significant shortcomings.

Weighting and Conclusion

Shortcomings underlined under the conclusion to R.10 with regard to the scope of application of the DDA (and consequently regulation and supervision) are also relevant here.

The E-Money Act and Payment Services Act do not provide a sufficiently clear basis for excluding criminals from ownership or management; however, these sectors are not material. Information has not been provided by the authorities on the application of market entry requirements to investment funds (which are FIs), where persons other than those authorised in respect of the

manager may hold management functions for corporate funds. This is considered to be a minor shortcoming on the basis that the managers of such funds are licenced by the FMA for prudential purposes.

Given that the last core principle assessments date back to 2008, the authorities have not clearly demonstrated that regulation and supervision of core principle institutions are in line with the relevant core principles. This is considered to be minor shortcoming.

R.26 is rated LC.

Recommendation 27 – Powers of supervisors

Liechtenstein was assessed LC for R.29 in the 2014 MER. The report noted that there were no specific provisions allowing the FMA to ensure that FIs apply AML/CFT measures consistent with FATF Recommendations across financial groups.

The introduction to R.10 lists activities to which the DDA does not apply and so which are not subject to regulation or supervision.

Criterion 27.1 – Supervisory authorities are responsible for ensuring compliance with execution of the DDA and implementation of Regulation (EU) 2015/847 (DDA, Art. 23). The FMA is the supervisory authority in relation to all covered FIs. Powers necessary to exercise supervision include the power to obtain information and documents and the power to conduct both ordinary (regular) and extraordinary inspections of supervised persons (DDA, Art. 28).

The FMA is also responsible for supervision of covered FIs compliance with TFS (ISA, Art. 5a and 5b). For this purpose, it may carry out ordinary and extraordinary inspections in line with powers given under the DDA.

Criterion 27.2 – Supervisory authorities have the authority to conduct inspections of covered FIs (DDA, Art. 28 (1)(b) and (c)): (i) ordinary inspections under Art. 24(1) DDA – to check compliance with the DDA; and (ii) extraordinary inspections under Art. 25 DDA – where there are doubts that due diligence requirements (set out in the DDA, DDO, FMA-Guidelines, FMA-Instructions and FMA-Communications) are being met or if circumstances exist that appear to endanger the reputation of the financial centre. They may also order that such inspections be conducted by mandated audit firms. The same powers are available to conduct inspections to supervise compliance with TFS (ISA, Art. 5b). The FMA has no similar powers to conduct inspections to supervise compliance with Regulation (EU) 2015/847 and instead the supervisor relies on a general provision that requires it to take measures in order to ensure compliance therewith (DDA, Art. 23(2)).

The term "circumstances exist that appear to endanger the reputation of the financial centre" is not defined.

Criterion 27.3 – Covered FIs must provide to the supervisory authorities, on request, all information and records required to perform oversight functions in accordance with the DDA (DDA, Art. 28(4)). Non-compliance may result in a fine of up to CHF 200 000 (DDA, Art. 31(1)(a)).

Covered FIs must, upon request, provide the supervisory authorities with all information, documents, and copies that they require to fulfil their responsibilities under the ISA (ISA, Art. 2b).

Criterion 27.4 – Supervisory authorities have a number of "supervisory measures" available to them (DDA, Art. 28 (1) (d) to (k)). They may: (i) prohibit the commencement of new business relationships for a limited period of time; (ii) order the discontinuation of a practice that violates the provisions of the DDA or Regulation (EU) 2015/847; (iii) publicly disclose decisions in the event of repeated, systematic or serious violations of the DDA or Regulation (EU) 2015/847; (iv)

temporarily prohibit (suspend) the performance of an activity it has authorised under sectorial legislation in the event of repeated, systematic or serious violations of the DDA or Regulation (EU) 2015/847 (a form of restriction on a licence); (v) withdraw the authorisation that it has granted under sectoral legislation in the event of repeated, systematic or serious violations of the DDA or Regulation (EU) 2015/847; and (vi) temporarily prohibit individuals from performing executive functions in the event of repeated, systematic or serious violations of the DDA or Regulation (EU) 2015/847. Non-compliance with a requirement of the DDA or Regulation (EU) 2015/847 may also be sanctioned by a fine of up to CHF 200 000 (DDA, Art. 31(1)(a)).

In addition, supervisory authorities may impose financial penalties based on a scale. The highest fine of up to CHF 5 million (or 10% of annual turnover in the case of a legal person) applies to breaches committed "substantially, repeatedly or systematically" by FIs (DDA, Art. 31). The FMA's enforcement policy and guidance explains that this covers offences that respectively: (i) have a material impact in respect of the concerned obligation and therefore can be described as grievous in the context of an overall assessment; (ii) are repeated more than twice; or (iii) involve a degree of planning or intentional behaviour. In the case of a combination of several criminal offences, only one penalty will be imposed (the principle of absorption), and the combination of several criminal offences represents an aggravating circumstance.

The circumstances in which these highest financial penalties may be applied to legal persons is limited to cases in which: (i) offences have been committed by senior management; and (ii) offences committed by employees which were made possible or considerably facilitated by senior management through failure to take necessary and reasonable measures. In the case of a first offence, the authorities have explained that, according to a rule for calculating the level of a fine set by the FMA Complaints Commission, the penalty may be limited to 10% of the maximum penalty (i.e., CHF 500 000).

A "limitation period" applies to the application of fines (administrative offences) – see c.35.1.

The range of sanctions set out in law is proportionate and allows a graduated range of sanctions to be applied to increasingly serious breaches of obligations. However, the reduced maximum penalty that may be applied to first offenders means that the range in such a circumstance may not be sufficiently proportionate.

In respect of TFS, supervisory authorities may take the "necessary measures to restore a lawful state of affairs" and apply financial penalties (ISA, Art. 5b). Art. 11(1a) provides for fines up to CHF 200 000 in cases where a FI fails to: (i) verify customer and transaction-related documents; or (ii) take the necessary organisational measures and ensure appropriate internal control and monitoring measures.

Each of the sectoral laws also provide the FMA with a power to withdraw registration in case of violation of the DDA, Regulation (EU) 2015/847 or the ISA (AIFM Act, Art. 51(1)(d) - systematic and serious violations of legal obligations; Asset Management Act, Art. 31(1)(d) – violation of legal obligations in a serious way; Banking Act, Art. 28(1)(e) – systematic or repeated violations of legal obligations; E-Money Act, Art. 20(1)(b) – systematic and serious violations of legal obligations; Insurance Distribution Act, Art. 62(1) – serious failure to apply supervisory requirements or official orders (legal obligations); Insurance Supervision Act, Art. 128(1) – serious failure to apply supervisory requirements or official orders (legal obligations); Investment Undertakings Act, Art. 38(1)(d) - systematic and serious violations of legal obligations; Payment Services Act, Art. 14(1)(c) – systematic and serious violations of legal obligations; and UCITS Act, Art. 28(1)(d) - systematic and serious violations of legal obligations). The Insurance Distribution Act and Insurance Supervision Acts also provide the FMA with a power to restrict a licence.

Weighting and Conclusion

Whilst the FMA does not have an explicit power to conduct inspections to ensure compliance with Regulation (EU) 2015/847, it is required to take measures that are considered to have the same effect. Accordingly, this deficiency is considered minor. Whilst the reduced maximum penalty that may be applied to first offenders (by virtue of a "rule") means that the range of sanctions may not be sufficiently proportionate, the penalty set in the law itself is considered to be proportionate and so this shortcoming is considered to be minor.

Shortcomings underlined under the conclusion to R.10 with regard to the scope of application of the DDA (and consequently regulation and supervision) are also relevant here.

R.27 is rated LC.

Recommendation 28 – Regulation and supervision of DNFBPs

Liechtenstein was rated LC for former R.24 in the 2014 MER. The report noted significant gaps in available sanctions and absence of the concept of corporate liability.

R.22 lists activities to which the DDA does not apply and so which are not subject to regulation or supervision.

Criterion 28.1 – Casinos and providers of online gambling (gambling games offered via means of electronic communication, especially the internet, telephone, television, radio, or other electronic media) licensed under the Gambling Act fall under the scope of the AML/CFT framework (DDA, Art. 3(1)(l)). The FMA is the responsible authority for AML/CFT supervision (DDA, Art. 23(1)(a)).

a) (Met) – Land-based casinos require a licence (Gambling Act (GA), Art. 8 to 17a and Casino Ordinance (CO), Art. 3 to 21). Online gambling licensing requirements are set out in Art. 60 to Art. 72 of the Gambling Act.

There is currently a moratorium on online activities – a government decision from 2011 states that all applications concerning online gaming licences will be suspended until the end of 2023. This prevents the issue of licences. No licences have been granted historically.

b) (Mostly Met) The Office of Economic Affairs is the competent authority for licensing (and for supervision of compliance with non-AML/CFT obligations) of casinos (GA, Art. 8 in conjunction with Art. 78(1)(a)). For a licence to be granted, it must be established that: (i) the applicant; (ii) its main commercial partners - meaning the persons bound by a contract or with a significant financial interest, or likely to influence the running of the gambling (CO, Art. 5); and (iii) its BOs - persons directly or indirectly having 5% of share capital or voting rights (CO, Art. 6 (1)), have a "good reputation" and are fit and proper (GA, Art. 9(b)). Directors and key function holders have to submit a dossier (CO, Art. 7a (2)) including extracts from the criminal register and garnishment register (original and not older than 3 months).

Inter alia, the licence holder must notify the Office of Economics in a timely manner before all significant changes to licensing conditions become legally effective, including: (i) any transfers of shares leading to a concentration of more than 5% of the capital or votes in the same hands; and (ii) agreements with important business partners, (GA, Art. 16)(b)). Changes of directors and key function holders must be notified to the Office of Economic Affairs no later than the date on which the person takes up the position (Casino Ordinance, Art. 7c).

The licence holder must notify the Office of Economic Affairs without delay, but at the latest within four weeks, of any criminal proceedings or criminal judgments initiated or carried out against the licence-holder, its governing bodies, shareholders, or BOs of shares, in Liechtenstein or abroad (GA, Art. 16(a)). The courts and OPP must notify the executing authorities without delay of the initiation and discontinuation of criminal, bankruptcy, or disciplinary proceedings

against operators of gambling games and their general managers (GA, Art. 81). In addition, directors and key function holders have to update their dossier every three years (Casino Ordinance, Art. 7b).

The Office of Economic Affairs may request further documents where it deems this necessary as evidence of good repute (CO, Art. 7a (6)). With regard to capital, the Office of Economic Affairs requests proof of the legitimate origin of funds (GA, Art. 9b (1)).

If an applicant to hold a significant or controlling interest is an associate of a criminal, this will be relevant to an assessment of "good reputation". Similar provisions do not apply to directors and key function holders that are associates of criminals.

c) (Met) – The responsibility for oversight of casinos' compliance with the AML/CFT framework lies with the FMA (DDA, Art. 23(1)(a)).

Criterion 28.2 – The FMA is the supervisory authority in relation to all covered DNFBPs except lawyers and law firms (DDA, Art. 23 (1) (a)). Lawyers and law firms are supervised by the Chamber of Lawyers (DDA, Art. 23 (1) (b)).

The Chamber of Lawyers, as a self-regulatory body, is under the supervision of the Government in relation to its AML/CFT supervisory functions, though this is limited to reviewing the legality of its administrative management (Lawyers Act, Art. 91(2)). Whilst this does not appear to also cover effectiveness or efficiency, decisions, and decrees of the board of the Chamber of Lawyers may be appealed, by way of objection, to the Government within 14 days of service, in which case a legal advisor in the Office of Justice examines the legal situation and prepares a decision in consultation with the senior advisor to the minister.

Criterion 28.3 – Covered DNFBPs are within the scope of the DDA (DDA, Art. 3). As such, supervisory authorities must monitor and supervise for compliance with the AML/CFT framework (DDA and ISA). The system for monitoring compliance must be risk-based (DDA, Art. 23a) and consists of ordinary and extraordinary inspections (DDA, Art. 24 and 25).

Criterion 28.4 – a) The same powers are available to supervise covered DNFBPs as for covered FIs – see c.27.1 to c.27.3.

b) *Trustees and trust companies:* A licence to act as a TCSP shall be granted upon application if shareholders, partners or persons holding a qualifying interest (25% or more of capital or voting rights) in the trust company satisfy the requirements established in the interests of "sound and prudent" management (Trustee Act, Art. 14(1)(d) in conjunction with Art. 3 (1)(d)). The term "sound and prudent management" is not defined, but, in practice, the authorities explain that shareholders must prove trustworthiness, which, inter alia, includes the absence of a criminal record. Members of management of the TCSP must be named and must be trustworthy (Trustee Act, Art. 14(1)(e) in conjunction with Art. 6). To prove trustworthiness, inter alia, absence of a criminal record must be demonstrated. It is not clear what statutory provisions are in place to deal with associates of criminals.

Any change in qualified participation or the management of a trust company requires prior approval from the FMA (Trustee Act, Art. 22(2)). Checks on shareholders subsequent to application are also conducted where there are indications that requirements are being breached.

An individual who applies to be a trustee must be trustworthy (Trustee Act, Art. 6).

To exercise an activity as an Art. 180a Act person, a licence issued by the FMA is required (180a Act, Art. 3(1)). A licence is only issued to natural persons where the respective person is a full-time employee with a trustee or trust company (180a Act, Art. 4(1)(d)). Inter alia, when applying for a licence the applicant must demonstrate trustworthiness (180a Act, Art. 4(1)(c) in conjunction with Art. 6), including absence of a final conviction for a misdemeanour or crime.

There is an obligation to inform the FMA immediately and in writing of any change in the circumstances on which authorisation is based, in particular changes that are required for the assessment of trust-worthiness pursuant to Art. 6 (Trustee Act, Art. 22 (1) and 180a Act, Art.11 (1)). The Courts must also communicate all decisions of a disciplinary or criminal nature to the FMA without being asked to do so and the OPP must inform the FMA of the opening and discontinuation of criminal proceedings and provide information concerning these proceedings (Trustee Act, Art. 58 and 180a Act, Art. 19(2) and (3)).

As part of their licence, TCSPs are authorised by the FMA also to provide tax advice and accounting services to their customers, without a requirement for them also to be separately licenced by the Office of Economic Affairs to provide these services.

Lawyers and law firms: Only lawyers entered into the Liechtenstein register of lawyers can be partners in a law firm (Lawyers Act, Art. 36). In addition, lawyers are prohibited from holding shares, stocks, or capital contributions for the account of third parties, and third parties may not participate in the profits of a law firm (Lawyers Act, Art. 36).

When applying for admission to the register, every lawyer must demonstrate "trustworthiness". Whilst there is no explicit reference to the need to demonstrate the absence of a criminal record in order to support trustworthiness (Lawyers Act, Art. 3(2)(b)), a current extract from the criminal register must be enclosed with an application for admission to the lawyers' examination (Lawyers' Examination Ordinance, Art. 3(2)(b)). In practice, applicants submit to the Chamber of Lawyers also a personal declaration that they are not aware of any pending criminal proceedings. In addition, they are expected to inform the Chamber of Lawyers immediately of any changes in their situation under a provision requiring the profession to act truthfully and honourably (Lawyers Act, Art. 12). If criminal proceedings are initiated against a lawyer, the criminal authorities are obliged to report this to the disciplinary authority of the Chamber (Lawyers Act, Art. 50).

It is not clear what statutory provisions are in place to deal with associates of criminals.

Other types of DNFBPs: "Reliability checks" are conducted by the Office of Economic Affairs (Business Act, Art. 11(1)(b) (in conjunction with Art. 12 and Art. 17 to Art. 19). These "reliability checks" are applied to: (i) in the case of a legal person, the holder of a qualifying holding (those with a holding of 25% or more), the managing director and any operations manager; (ii) in the case of a natural person, that person and any operations manager. In all cases, an original criminal register extract must be provided (Business Act, Art. 26). The person licenced to trade or managing director must notify the Office of Economic Affairs immediately in writing if there is a subsequent change in circumstances (Business Act, Art. 23). It is not clear what statutory provisions are in place to deal with associates of criminals.

c) Supervisors may apply "supervisory measures" (DDA, Art. 28(1)) and fines for administrative offences (DDA, Art. 31). See c.27.4 and c.35.1.

These are in line with measures and fines available for FIs under the DDA and ISA, except that the highest fine available for covered DNFBPs under the DDA is up to CHF 1 million (or 10% of annual turnover) which applies to breaches committed "substantially, repeatedly or systematically" (DDA, Art. 31) a term that is defined in the FMA's enforcement policy and guidance (see c.27.4). In the case of a combination of several criminal offences, only one penalty will be imposed (the principle of absorption), and the combination of several criminal offences represents an aggravating circumstance.

The circumstances in which these highest financial penalties may be applied to legal persons is limited to cases in which: (i) offences have been committed by senior management; and (ii) offences committed by employees which were made possible or considerably facilitated by senior management through failure to take necessary and reasonable measures. In the case of a first

offence, the authorities have explained that the highest penalty may be limited to 10% of the maximum penalty (i.e., CHF 100 000) based on rules set by the FMA Complaints Commission – see c.27.4.

A "limitation period" applies to the application of fines (administrative offences) – see c.35.1.

The range of sanctions set out in law is proportionate and allows a graduated range of sanctions to be applied to increasingly serious breaches of obligations. However, the reduced maximum penalty that may be applied to first offenders means that the range in such a circumstance is not considered to be sufficiently proportionate, particularly for TCSPs, where information on profitability has not been provided to the AT.

Criterion 28.5 – The analysis under c.26.5 applies equally to covered DNFBPs. The only substantive difference in approach is that the supervisory authorities may create a sector risk profile instead of an individual risk profile for entities in that sector, when the risk in a particular sector is determined as minor or moderate in the NRA (DDA, Art. 23a (3)). This is the case for dealers in goods, real estate agents, external bookkeepers, and members of tax consultancy professions.

The authorities have not explained what systems are in place to identify any DNFBP groups based in Liechtenstein that may present a higher ML/TF risk and effect that such an assessment may have on supervision of the parent company (distinct from supervision of the group).

Weighting and Conclusion

A combination of the following is considered to present moderate shortcomings: (i) it is not clear what statutory provisions are in place to deal with associates of criminals; and (ii) the reduced maximum fine that may be applied to first offenders - which means that the range of sanctions that may be applied for failing to comply with the DDA is not considered to be sufficiently proportionate.

Shortcomings underlined under the conclusion to R.22 with regard to the scope of application of the DDA (and consequently regulation and supervision) are also relevant here. **R.28 is rated PC**

Recommendation 29 - Financial intelligence units

In the 4th MER, Liechtenstein was rated PC for the former R.26. A number of deficiencies were identified in relation to the FIU's access to information. Various restrictions in this regard included: (i) the power to obtain information is subject to secrecy provisions; (ii) the FMA had several limitations for provision of confidential information to the FIU; (iii) there was no clear obligation for the FMA or law enforcement to provide the FIU with the requested information; and (iv) the FIU's power to obtain additional information from persons subject to the DDA could be restricted. Finally, these restrictions have also had an impact on the FIU's adherence to the Egmont Group's Principles for Information Exchange.

However, the 2018 follow up report concluded that after the adoption of the MER, all these deficiencies had been addressed and mitigated.

Criterion 29.1 – Liechtenstein's FIU is an independent administrative-type FIU within the Ministry of General Government Affairs and Finance. The FIU is the central national agency for receipt and analysis of information that is required for the detection of ML, predicate offences to ML, organised crime and the TF (FIU Act, Art. 3 (1)). The FIU guidance stipulates, that the main responsibilities of the FIU are receiving and analysing reports and other relevant information in the area of combating ML, predicate offences to ML, TF, and organised crime.

FIU has core and additional responsibilities. The core responsibilities include (a) receiving information from public and non-public sources within the remit of its function; (b) analysis of information to determine whether the suspicion of ML, predicate offences to ML, organised crime or TF can be confirmed on the basis of such information; (c) delivery of analytical reports, as well as any other relevant information to the Public Prosecution Service in the event of a reasonable suspicion that ML, predicate offences to ML, organised crime or TF were committed. The analytical report shall not contain any details about the source of the information or disclosure. (FIU Act, Art. 4).

Criterion 29.2 –

(a) Where a suspicion of ML, predicate offence to ML, organised crime or TF exists, the persons subject to the DDA must immediately report it to the FIU in writing; the responsibility for submitting reports stands with the member appointed at executive level to ensure compliance with the Act (DDA, Art. 17). FIU receives information from public and non-public sources within the remits of its function (FIU Act, Art. 4 (a)) - see also c.29.1.

(b) The reporting regime stipulated in Art. 17DDA does not foresee any other reporting requirements apart from STRs/SARs.

Criterion 29.3 –

(a) FIU has the power to require persons subject to the DDA to provide information for analytical purposes, insofar as the information has been documented. The disclosure request from the FIU shall take precedence over all obligations of confidentiality recognised by the Government. (FIU Act, Art. 5a (1) (b); DDA, Art. 19a (1 and 2)).

In addition, FIU may, for statistical purposes, require persons subject to the DDA to provide non-personal data concerning business relationships. Statutory provisions on the protection of confidentiality are reserved. (FIU Act, Art. 5a (1) (c)).

FIU is empowered to use information received from public and non-public sources to determine whether the suspicion of ML, predicate offences to ML, organised crime or TF can be confirmed on the basis of such information (FIU Act, Art. 4)

(b) FIU has the powers to collect financial, administrative and law enforcement information from other official agencies and the FMA, insofar as such information is available. These bodies are obliged to provide the FIU with the information requested immediately as far as this is permissible (FIU Act, Art. 5a (1) (a)).

Criterion 29.4 - FIU's competencies to conduct operational and statistical analysis are covered within the core and additional responsibilities of the FIU (FIU Act, Art. 4, 5 and 5a).

(a) For operational analysis, FIU has the following responsibilities (i) receiving information from public and non-public sources within the remit of its function; (ii) analysing of information to determine whether the suspicion of ML, predicate offences to ML, organised crime or TF can be confirmed on the basis of such information; (iii) producing and delivering analytical reports, as well as any other additional relevant information, to the Public Prosecution Service in the event of a reasonable suspicion of ML, predicate offences to ML, organised crime or TF.

(b) The provisions for conducting strategic analysis are embedded in Art. 5 of the FIU Act. They explicitly require the FIU to '*carry out analysis of general threats from money laundering, predicate offences to money laundering, organised crime and terrorist financing'* in course of which it may consult other competent authorities and persons subject to the DDA. As a result, the FIU should prepare reports, independently from the Government, the FMA, other agencies or professional associations, assessing the specific ML/TF threats (Art. 5 (c)).

Criterion 29.5 - FIU delivers a report containing the results of the analysis, as well as any other additional information, to the Public Prosecution Service in the event of a reasonable suspicion of ML, predicate offences to ML, organised crime or TF. This report shall not contain any details about the source of the information or disclosure (FIU Act, Art. 4 (c)).

The FIU may exchange financial, administrative and law enforcement information and relevant documents required for the prevention of ML, predicate offences to ML, organised crime and TF with other domestic authorities, in particular the courts, Public Prosecution Service, National Police, Office of Justice, Tax Authority and FMA. (FIU Act, Art. 6 (1)). Dissemination of information upon request is provided under Art. 36(1) of the DDA, whereas all authorities are obliged to exchange necessary information upon request within the framework of the DDA.

The FIU is authorised to process personal data, including particular categories of personal data and personal data concerning criminal convictions and offences, and to create profiles, insofar as this is necessary for the performance of its statutory function. This data may only be processed for the purpose for which it was collected. (FIU Act, Art. 8(1)(2)).

The Government may establish more specific regulations on data processing by ordinance, in particular concerning: a) measures to guarantee the secure communication of data; b) access to the data, processing authorisation, storage of the data, archiving and deletion of data, as well as data security. (FIU Act, Art. 8(4)). In order to perform its function, the FIU may operate electronic information systems that may contain the data referred to in Art. 8 (FIU Act, Art. 8a).

The FIU may disclose or communicate personal data, including particular categories of personal data and personal data concerning criminal convictions and offences, as well as data from profiling to offices of the national government, administrative authorities and courts, as well as foreign FIUs, insofar as this is necessary for the performance of its statutory duties or the duties of the recipients of the data (FIU Act, Art. 8c).

The authorities advised that disseminations to the FMA are sent via a secure reporting platform (goAML – secure message board) and starting from June 2021, disseminations to the Public Prosecutor`s Office for law enforcement action and disseminations to Tax Authority are also sent via the goAML message board. Before June 2021, the channel to disseminate information between the FIU and the OPP was internal postal service/courier. FIU also exchanges information with Office of Justice, however no information is provided on the channel of information exchange.

Criterion 29.6 - (a) The FIU shall guarantee the protection of its sources and preserve their anonymity, in particular the anonymity of persons subject to the DDA who have disclosed information or who have complied with a request for information from the FIU (Art. 11b, FIU Act).

(a) Procedures for handling, storing, disseminations as well as protection and access to information are stipulated in the Analysis Manual, which all staff members are to comply with when conducting analytical work and accessing data and information from available data sources and storage. In accordance with the Manual, at several instances during various kinds of analytical scenarios (i.e., handling an SAR/STR, requesting information from authorities/persons subject to the DDA, handling a request from an international counterpart etc.), specific workflow is to be applied via goAML platform. This workflow requires that either the head of the FIU, the head of the operational analysis or the deputy head or the head of the strategic analysis department are involved and consulted before information and data is transmitted to third parties.

(b) Both the FIU staff and internal postal service staff are bound to Art. 38 of State Personnel Act. (1) Employees are obliged to maintain secrecy about official matters which by their nature or according to special regulations must be kept secret. This obligation shall remain in force even after termination of the employment relationship. (2) Subject to other statutory provisions, official communications within the administration and the provision of information to superiors

and supervisory bodies are exempt from the duty of confidentiality. (3) Employees may only speak as parties, witnesses and judicial experts on official matters that are subject to the duty of confidentiality if they are authorized to do so in writing by the head of the office. (4) Authorization shall be granted if the statement would not cause any significant harm to the welfare of the country and would not seriously jeopardize or significantly impede the performance of public duties (State Personal Act, Art. 38 (1-4)).

(c) The FIU`s internal IT infrastructure ensures extremely limited access to the FIU`s data pools (goAML test environment, goAML production environment, FINETO environment [old database prior to goAML] etc.). The so-called "FIU Zone" is detached from the general IT zone which is administered by the Office for Information Technology. The FIU zone is accessed by FIU IT-staff and in cases of utmost urgency and need there is one dedicated IT-Officer within the Office for Information Technology who could access the FIU zone as well, if required by the Head of the FIU or his deputies.

There is also a physical access control policy is implemented in the entire State Administration. All employees are granted access via electronic key card only to the areas necessary to fulfil their employment. When physical access authorisations are taken with meticulous care is taken to ensure that only employees of the relevant office can gain access. The definition of who requires access to which office building/room is defined directly by the Director of each office and forwarded to the Office of Construction and Infrastructure for implementation.

The FIU`s premises can only be accessed by FIU staff using an electronic key card. Its IT is managed by the administration`s IT department and servers are located within the department`s facilities in Vaduz, while maintaining a separate LAN security zone dedicated to the FIU.

Criterion 29.7 **-** (a) FIU is independent in the performance of its core responsibilities – receiving, analysing and disseminating these analysis to the competent authorities (FIU Act, Art. 4), as well as in carrying out several other responsibilities, that include analysis of general threats from ML, predicate offences to ML, organised crime and TF and analysis of information to determine whether such information indicates patterns for the existence of criminal offences of that nature (FIU Act, Art. 5 a and b; FIU Act, Art. 3(2)).

(b) After consulting the competent member of the Government the FIU may conclude (i) agreements with other domestic authorities on the arrangements for the cooperation (FIU Act, Art. 6(4)); (ii)agreements with foreign FIUs on the arrangements for the cooperation (FIU Act, Art. 7(4)).

The provision which conditions "concluding agreements after consultation with the Government" appears not to be in line with this FATF Recommendation which concerns the FIU's independence. Authorities advise, that said MoUs with foreign counterparts are not required by the FIU and there is no negative impact of having this provision in the law, as the Government has never declined to have the FIU sign a MoU with a foreign counterpart. With the purpose of technical compliance, this provision largely concerns FIU's independence.

(c) The FIU is not located within an existing structure of another authority. In terms of the overall governmental organizational structure, the FIU is defined as a "Stabsstelle", i.e., an administrative unit within the Ministry for General Government Affairs and Finance. However, it does not share premises nor staff with the said ministry and has very distinct and unique functions within the overall governmental structure.

(d) FIU obtains and deploys the resources needed to carry out its functions based on the approval of Ministry for General Government Affairs and Finance.

Criterion 29.8 – Liechtenstein's FIU has been a full Egmont Group member since 2001.

Weighting and Conclusion

FIU is independent and autonomous in conducting its core and several additional responsibilities, however, for domestic and international cooperation, FIU may conclude agreements only after consulting with competent government member. This, from the technical compliance point, in its turn undermines the overall independence of the FIU.

R.29 is rated LC.

Recommendation 30 – Responsibilities of law enforcement and investigative authorities

In the 4th round of MER in 2014, responsibilities of law enforcement and investigative authorities were not under the scope of investigation. In the 3rd round of MER in 2008 the law enforcement authorities had been rated LC, only questioning the effectiveness since no ML convictions were to be found stating that this might be a result of the absence of autonomous ML prosecutions.

Criterion 30.1 –Investigative judges at the Court of Justice, the OPP and the National Police (the Economic Crime Unit is specialized in investigating financial crimes including ML, associated predicate offences and TF) are responsible for criminal investigations in general.

The Office of the Public Prosecutor is ultimately responsible for an investigation and the prosecution of ML, associated predicate offences and TF offences in accordance with Art. 20 to 22 CPC. In an investigation, prosecutor can request investigating judge to order specific coercive measures (e.g., search and arrest warrants), in which case the prosecutor remains in charge of the proceedings ("Vorerhebungen"; Art. 21a CPC). If, upon prosecutor's request, an investigating judge decides, by way of a ruling, to initiate an investigation ("Untersuchung"; Art. 41 and 42 CPC) then the investigative judge is required to investigate the crime on his/her own whereas no further requests/applications by the prosecutor are required. In practice, these investigations are either triggered by FIU reports or MLA requests or direct police investigations.

The prosecutor and the investigating judge conduct the investigations with support provided by the National Police, and in particular for cases of ML, associated predicate offences and TF, their Economic Crimes Unit which possesses the expertise necessary for such special investigations. If there is a suspicion that a criminal offence (including ML and TF) occurred, the law enforcement authorities are obliged to conduct an investigation.

Furthermore, the National Police have to carry out inquiries on its own initiative (Art. 9 to 11 CPC).

Criterion 30.2 – Authorities advised that the law enforcement authorities, especially the OPP and the National Police (Economic Crime Unit), are also responsible for parallel financial investigations and asset recovery measures, regardless of where the predicate offence is committed (provided that the offence committed abroad would constitute a criminal offence under Liechtenstein law).

Whereas the legislation provides for general investigative prerogatives of the OPP (Art. 21 (1) CPC; Art. 21a CPC) and the National Police (Art. 10 (1) CPC), the practice and also the objectives set up in the asset recovery strategy consider confiscation as a primary objective – an objective which should be attained through application of available investigative means, whereby all possibilities provided throughout the criminal proceedings are to be exhausted. Therefore, the understanding of the competent authorities is that parallel financial investigations have to be carried out regularly in order to detect any (further) assets generated through the commission of criminal offence(s).

Criterion 30.3 – The Liechtenstein law enforcement authorities are obliged to identify, trace, freeze and initiate seizing of property that is or may become subject to confiscation/forfeiture or

is suspected of being proceeds of crime (see R.4). The National Police and the Public Prosecutor are competent authorities within the meaning of this essential criterion (Art. 9, Art. 10 and Art. 96a of the CPC).

Liechtenstein has also issued guidelines for practitioners on pecuniary orders. These guidelines were prepared by the OPP and are published at the homepage of the StAR initiative (https://star.worldbank.org/sites/star/files/guidelines_on_pecuniary_orders_2018_en.docx).

Criterion 30.4 – Since there are no other competent authorities which are not LEAs, and which have responsibility for conducting financial investigations into predicate offences, this criterion is not applicable.

Criterion 30.5 – There is no separate special anti-corruption enforcement authority in Liechtenstein. The National Police (four special agents of the Economic Crime Unit) pursuant to Art. 9 to 11 and 21a CPC are also responsible to investigate corruption offences and ML/TF related to corruption offences. This unit of the National Police directly reports to the OPP.

Weighting and Conclusion

R30 is rated C.

Recommendation 31 - Powers of law enforcement and investigative authorities

In respect of powers of the competent authorities Liechtenstein was rated compliant (C) in the 3rd round of MER in 2008 (omitting this aspect in the 4th round MER of 2014).

Criterion 31.1 – The competent authorities investigating ML, associated predicate offences and offences in connection with organised crime are able to obtain access to all necessary documents and information for purposes of these investigations, prosecutions, and related actions. Art. 96b of the CPC, which regulates this matter also (though indirectly) refers to TF since the TF is a predicate offence to ML (see also R.5).

a) Art. 96b (1) CPC empowers the Court of Justice to query all persons subject to the DDA insofar as this appears necessary ***to solve a case of money laundering as defined in the CC, a predicate offence to money laundering, or an offence in connection with organized crime*****,** to:

> 1. disclose the name, other data known to them about the identity of the holder of a business relationship and the contracting party, and such persons' address;
>
> 2. disclose whether a suspect maintains a business relationship with the person subject to the DDA, is a BO or authorised person of such business relationship, and, to the extent this is the case, provide all information necessary to identify that business relationship and deliver all materials concerning the identity of the holder of the business relationship and the person's power of disposal; and
>
> 3. surrender all documents and other material concerning the type and scope of the business relationship as well as business transactions and other business events related to such business relationship from past or future period of time. The same applies in situations where a business relationship was or is being used for the transaction of a pecuniary advantage that is subject to forfeiture (Art. 20 CC) or extended forfeiture (Art. 20b CC). For seizure of documents held by other entities, the procedure according to Art. 96 CPC is applied for all items that may be relevant to the investigation (evidence) or subject to confiscation. This is either preceded by a search warrant (Art. 92 CPC) or by a request of the judge pursuant to Art. 96 (2) CPC (*everybody is obliged to hand over on request any items that are to be seized, in particular documents*). The obligation to surrender the requested documents or other relevant items or values is enforceable by the judge; any person

refusing is liable to a fine of CHF 10 000 or imprisonment of up to six weeks, except if she/he is the suspect himself or if she/he is absolved to testify (Art. 96(2) CPC).

Art. 96(1) CPC extends to all items and information stored on data carriers that may be of importance for the investigation (evidence) or are subject to confiscation or deprivation order, forfeiture or extended forfeiture of assets. Art. 96 (1) CPC also provides a possibility to seize VAs, in particular virtual currencies or cryptocurrencies. According to the explanatory memorandum, the law enforcement authorities are free to choose their course of action under Art. 92, 96 and 96b CPC.

b) House and personal searches, including premises and vehicles, are conducted according to Art. 92 CPC. As a rule, this is based on a search warrant issued by the investigating judge, but can also be performed by the National Police on their own initiative in certain circumstances (Art. 94 CPC): if it has been ordered by the judge that a person be brought before the court or arrested, or where a person is caught in the act, is made suspect of a punishable act by public pursuit or public call, or is found to be in possession of items that indicate participation in a punishable act.

c) Pursuant to Art. 105 CPC a witness is obliged to follow the summoning of the law enforcement authorities. Witnesses are also obliged to give full and truthful testimony.

Certain persons are exempted from testifying or have legally granted rights to refuse to testify pursuant to the provisions set forth in Art. 106 to 108 CPC. These exemptions are particularly relevant with certain DNFBPs such as lawyers and notaries. A specific issue on legal privilege (Art. 108 (2) CPC)) allows some persons to refuse to give testimony. Potential abuse of the legal privilege is countered by the Liechtenstein authorities with the presumption that a DNFBP is acting in its capacity of financial intermediary or other capacity of a professional subjected to the DDA. The burden of proof that the relevant information fall under this privilege, is on the subject which claims a right to this privilege. The case law confirmed that legal privilege of a lawyer (Art. 108 (2) 2 CPC) only applies if this person acts as a lawyer. If a lawyer acts as a trustee he has no legal privilege and in such situations authorities' capability to obtain information is not limited (decision of the Supreme Court OGH 07.05.1998; LES 1999, 37 and the Constitutional Court GH 1998/39; LES 2002, 70).

The right to refuse to testify must not be circumvented through the attachment and seizure of documents and of information stored on data carriers or through the examination of employees or persons who participate in the professional activity for training.

Witnesses located in Liechtenstein are, on threat of a fine of up to CHF 1 000 in the event of nonappearance, summoned by the National Police if they do not comply with the order to appear (Art. 113 CPC). If the witness is unwilling to testify the court can impose coercive measures (Art. 114 CPC). In principle, witnesses are subject to a coercive penalty of up to CHF1 000 and, in the event of continued refusal, coercive detention of up to six weeks. False testimony in court or before the National Police is punished by imprisonment of up to three years and perjury with imprisonment of six month up to five years (CC, Art. 288 (1) to (3)).

d) The seizure regime in Liechtenstein is based on Art. 96 CPC and 96b CPC (see c.31.1 a); these articles are used either for evidentiary purposes or to ensure effective confiscation. They require the involvement/approval by the court (i.e., the investigating judge). Pursuant to Art. 96a CPC the National Police are entitled to seize objects on their own initiative (see also c. 4.2 (b) and 31.1 a), b) and c)).

Criterion 31.2 – Competent authorities are able to use the following investigative techniques for the investigation of ML, associated predicate offences and TF ('*punishable acts committed with intent and subject to a penalty of more than one year imprisonment*'):

a) Pursuant to Art. 104b CPC, the National Police may on their own initiative employ their officers or other persons - who will neither disclose their official capacity or their mission nor let it be known (undercover investigation) - on their behalf if this may further the investigation of an offence. A systematic long-term undercover investigation carried out by the National Police must be approved by the investigating judge on application of the public prosecutor.

b) The surveillance of electronic communication can be ordered by the investigating judge pursuant to Art. 103 CPC, but he/she immediately has to obtain the approval of the President of the Court of Appeal. Ordering the surveillance of electronic communication including the recording of its content is admissible where it is to be expected that this will further the investigation and if *(1) the holder of the communication equipment (e.g. phone) is himself strongly suspect of having committed the offence, or (2) there are reasons to assume that a person strongly suspect of the offence is staying with the holder of the equipment or is going to contact him using the equipment or (3) the holder of the equipment expressly agrees to the surveillance.*

The surveillance is limited to three months; if the requirement of surveillance continues to exist after that period, the procedure can be repeated. The National Police is responsible for the implementation of the surveillance of electronic communication in cooperation with the providers in terms of the Communication Act. There is no notification of parties or other participants of the proceedings during the surveillance.

c) Competent authorities are empowered to access computer systems by seizing (Art. 96 (2a) CPC) electronic data carriers or keeping electronic communication under surveillance (Art. 103 CPC).

d) On application of the prosecutor and after a ruling to such effect has been issued by the investigating judge, the National Police has the right to conduct an undercover transaction pursuant to Art. 104c CPC (the attempted or apparent commission of offences as far as these consist in the acquisition, obtainment, holding, import, export, or transit of items or assets that have been stolen, originate from a crime or are dedicated to committing a crime, or whose possession is absolutely prohibited). Controlled delivery is also permissible pursuant Art. 9 CPC (investigating powers of the National Police) in connection with Art. 27 Narcotics Act (controlled sale or purchase of drugs by a law enforcement officer) and Art. 73 of the Schengen Agreement (controlled delivery of drugs).

Criterion 31.3 – a) Reference is being made to criterion 31.1 above. Art. 96b CPC is applicable to all persons subject to the DDA. This requirement covers all DNFBPs.

Institutions can be ordered to provide detailed information on the identity of persons and business relations, the nature of the relationship, the identity of the holder of the business relationship and his power of disposal as well as on the BOs and to surrender all documents and other material concerning the type and scope of the business relationship as well as business transactions and other business events related to such business relationship from a certain past or future period of time and supply all related documentation). As noted already, this requirement does not cover all DNFBPs.

Usually, the investigating judge orders the institutions to provide the information and documents within 14 days but in urgent cases the deadline may be shortened.

b) A ruling pursuant to Art. 96b CPC is served upon the entities as numerated in this article. Service to the other persons with power of disposal may be delayed as long as such service would endanger the purpose of the investigation. The entities pursuant to Art. 96b (3) CPC are notified of this and must for the time being maintain secrecy towards clients and third parties with respect to all facts and processes associated with the judicial order. Also, persons working for one of these entities must not inform the contract partner or third parties about a pending investigation. A violation of this prohibition of notification constitutes an offence under Art. 301 (2) CC.

Criterion 31.4 – The courts, the OPP and the National Police pursuant to Art. 8 (1) CPC are not only required to provide mutual administrative assistance for the performance of duties under the CPC but they are also entitled to request support from all authorities of the state and of the municipalities. These authorities have to execute such requests without unnecessary delay or have to immediately indicate any obstacles to their execution. Pursuant to Art. 6 (1) FIU-Act the FIU can share all relevant information and documents held by the FIU with competent authorities conducting investigations of ML, associated predicate offences and TF.

Weighting and Conclusion

R.31 is rated C.

Recommendation 32 – Cash Couriers

In the 4th round MER of 2014, Liechtenstein was rated PC on SRIX. The technical deficiencies identified were as follows: (i) it was not clear whether the disclosure system would apply in the case of shipment of currency through containerised cargo or to the mailing of currency; (ii) the conditions to seize were more restrictive/different than the FATF requirement to "stop or restrain"; (iii) sanctions were not proportionate and not applicable in the case of legal persons; (iv) shortcomings identified in connection with Recommendation 3 and Special Recommendation III applied in the context of Special Recommendation IX. The 2018 follow up report concluded that improvements have been noted on the sanctioning regime.

Criterion 32.1 **-** Liechtenstein adopted a disclosure system for cross-border transportation of currency and BNIs. To prevent and combat ML and TF, the National Police may, in the context of controlling cross-border cash transactions, demand information of persons concerning the following: a) the person questioned; b) the import, export and transit of cash in the amount of at least CHF 10 000 or the equivalent in a foreign currency; c) the origin and intended use of the cash; d) the BO (Police Act, Art. 25e (1)). In line with the FATF definition, the notion of cash includes: (i) cash in the form of banknotes or coins, irrespective of the currency, provided they are circulated as means of payment; and (ii) transferable bearer securities, shares, bonds, cheques, and similar securities (Police Act, Art. 25e(5)).

According to the Implementing Agreement of 18 December 2012 between the National Police and the Swiss Customs on Police Cooperation in the Border Area (hereinafter referred as 'Cash Control', Art. 1c(1)), the Swiss Border Guard Corps shall carry out cash controls at the Liechtenstein border crossing posts to Austria according to the Police Act, Art. 25 and Swiss Border Guard Corps rules. Liechtenstein is associated with the Swiss customs territory, of which it is an integral part. There is no customs department in Liechtenstein. Commercial cross-border movement all merchandise, including cash, is subject to a declaration system (Art. 25 and 26 Swiss Customs Law). According to the General terms and conditions (GTC) of Swiss and Liechtenstein Post, undeclared transportation of all merchandise, including cash, is prohibited. At that, customs clearance is conducted by Swiss Customs at mail distribution points. There is no declaration or disclosure system at the border between Switzerland and Liechtenstein. This lack of controls is based on the customs union treaty between both countries. Nonetheless, in the event of any suspected case of ML/TF, the competence to prosecute lies with the Liechtenstein authorities.

Criterion 32.2 **N/A**

Criterion 32.3 **-** The responsibility of travellers to provide truthful answers is ensured with the provision that, if incorrect information is provided or if information is withheld, the National

Police may provisionally secure cash in order to clarify whether a suspicion of a criminal offence exists (Police Act, Art. 25e (3)). The National Police is entitled to demand information only if the import, export, and transit of cash exceeds the amount CHF 10 000 or the equivalent in a foreign currency.

The secured objects or assets shall be logged in a register, which shall also indicate the reason for which they have been secured. A copy shall be given to the person concerned on request. As soon as the conditions for securing the objects or assets are no longer met, the National Police shall return the objects or assets to the entitled person (Police Act, Art. 25c (3,4)) - see also C.32.1.

Criterion 32.4 - There is no direct provision that entitles the National Police or other authorities to request further information from the carrier in case of false disclosure. However, if incorrect information is provided or if information is withheld, the National Police may provisionally secure cash in order to clarify whether a suspicion of a criminal offence exists (Police Act, Art. 25e (3)).

In the case of suspicion of ML or TF, the National Police may also demand information if the amount of the cash imported or to be imported to Liechtenstein, transited or exported, does not reach the threshold of CHF 10 000 or the equivalent in a foreign currency (Police Act, Art. 25e (2)).

The given provision does not entitle the Police to demand information in case of a false disclosure of the cash if the amount does not exceed CHF 10 000, which is not related to the suspicion of ML/TF or predicate offence.

Criterion 32.5 - If a person refuses to provide information on cash or provides false information, the National Police reports the case to the OPP. This is an infraction pursuant to Art. 36 (2) of the Police Act.

Anyone who refuses to provide information or provides false information in this regard shall be punished by the Court of Justice for committing a contravention and sentenced to a fine, or to imprisonment of up to one month if the fine cannot be collected. The fine shall amount to up to 30% of the value of the cash carried in Swiss francs if an infraction is committed by a legal person Art. 74a and 74d CC apply (Police Act, Art. 36 (2)).

The maximum fine amounts to up to 30% of the value of the cash carried and no minimal rate is stipulated. While there is no explicit alternative sanction in place for legal entities, if the convicted legal entity does not deposit the fine imposed pursuant to Art. 36 para 2 Police Act, immediately after the judgement has become final, the legal entity is asked in writing by the Court of Justice to pay this fine within 14 days on penalty of collection by coercion (Art. 249 para 1 and 4 CPC). If unsuccessful, a petition may be filed to initiate bankruptcy proceedings against the legal entity, which proceedings may end with the deletion of the legal entity from the commercial register. In addition, there is also possibility for dissolution of the legal person, in case it harms the national interests of the country.

Criterion 32.6 - The National Police shall, without delay, notify all cases of suspicion to the FIU and shall report such cases to the OPP (Police Act, Art. 25e(4)).

Criterion 32.7 - Authorities advise that adequate cooperation exists with the Swiss Border Guard Corps, National Police, the FIU and the OPP. In the case of dutiful provision of information and plausible assessment, merely the cash control form shall be transmitted to the National Police (Cash Control, Art. 1(c)(2)). If information as referred to in article 25e, paragraph 1 of the Police

Act is denied, wholly or partially, or in the case of false provision of information as well as initial suspicion of ML or TF on other grounds, the National Police shall be involved immediately and the cash control form provided (Cash Control, Art. 1(c) 3). See also C.32.6.

Criterion 32.8 **-** The authorities advise that the Swiss Customs Act (SCA) is applicable in Liechtenstein and empowers the Swiss Border Guard Corps to stop a person at the border and restrain goods and assets in order to fulfil their duties. Moreover, in line with Art. 104 (3) of the Swiss Customs Act, the Swiss Border Guard Corps is obliged to hand over the restrained/secured goods or assets to the competent authority (i.e., in this case it would be the National Police) immediately.

National Police is entitled to seize objects on their own initiative, if those objects a) are not subject to anyone's power of disposal, b) were taken from the injured party through the offence, c) were found at the scene of the offence and might have been used to commit the offence or might have been intended for that purpose, or d) are of little value or can easily be replaced on a temporary basis (CPC, Art. 96a(1)).

Moreover, the National Police can, based on Police Act Art. 25e(3), also seize objects if the possession of such objects is generally prohibited or if the objects are found on an arrested person or during a search that the National Police is permitted to carry out on their own accord (CPC, Art. 96a(2 and 3)).These provisions entitle the National Police to seize objects if incorrect information is provided or if information is withheld. The National Police may provisionally secure cash in order to clarify whether a suspicion of a criminal offence exists (Police Act, Art. 25e (3)) until seizure or freezing is ordered by the Court of Justice.

Criterion 32.9 **–**Art. 1C of the Implementing agreement of 18 December 2012 between Switzerland and Liechtenstein allows the competent authorities of Switzerland to transfer information on disclosure to the National Police. Furthermore, Art 35 of the Police Act authorises the National Police to exchange information with the competent foreign law enforcement authorities. This includes the information on cross border disclosures. The only exemptions from the information exchange as foreseen by Art. 35 are those which concern criminal matter relating to taxes, duties, customs, or foreign exchange (Art. 35 (3) (b) of the Police Act).

Personal data may be processed for as long as the data is necessary for performance of the task, but at the longest until expiry of the retention period laid down by the Government by ordinance; the data must then be deleted. (Police Act, 34e (1)). The authorities advised that the expiry of the storage period specified by the government by ordinance is basically at the longest ten years.

a) The court, the Prosecution Service and the National Police may, in the exercise of their duties, process the personal data required for that purpose where the provisions of the Data Protection Act (DSG) apply. The authorities shall preserve the protection-worthy interests in secrecy of the persons concerned and shall give priority to the confidential handling of the data. (CPC, 39a).

b and c) The National Police shall record their investigations in files, so that it is possible to verify the occasion, conduct, and result of such investigations. Grounds must be provided for the use of force and of powers that are connected with an infringement of rights, unless such grounds are already contained in the order from the Prosecution Service or the court. (CPC, Art. 11(1)). The National Police shall report to the Prosecution Service in writing if and as soon as (1) they learn of the suspicion of a serious crime or any other offence of particular public interest (incidence report) (CPC, Art. 11(2)(1)).

Criterion 32.10 **-** Requirements for the security of data processing include the implementation of necessary technical and organisational measures to ensure a level of security appropriate to the

risks inherent to personal data processing (Data Protection Act Art. 63(1)), in particular as regards the processing of special categories of personal data. These measures include pseudonymisation and encryption of personal data and should ensure: (i) the ongoing confidentiality, integrity, availability and resilience of processing systems and services in connection with processing; and (ii) the ability to restore the availability and the access to personal data in a timely manner in the event of a physical or technical incident (Data Protection Act, Art. 63 (2)).

With respect to automated processing, the controller and processor, following an evaluation of the risks, shall implement measures which include, but are not limited to, the prohibition of unauthorised access; the prevention of unauthorised reading, copying, modification or erasure of data media; the prevention of unauthorized inspection, modification, and deletion of data, etc. (Data Protection Act, Art. 63 (1) and (2)). Also, there is no obstacle limiting either trade payments between Liechtenstein and other countries, nor freedom of capital movements.

Criterion 32.11 **-** In principle, persons transporting currency or BNI related to ML/TF or predicate offences would be charged for ML/TF and thus would be subject to the same criminal sanctions as referred under R.3, in which case the general confiscation and provisional measures regime would be applicable to the respective currency or BNIs.

(a) Natural persons convicted of ML offences are subject to imprisonment of a term not exceeding three years (CC, Art. 165 (1) and (3) CC) or two years (Art. 165(2)).

Predicate offences to ML are all criminal offences punishable with more than one year imprisonment and a series of designated misdemeanours (one year or less than one year imprisonment - CC, Art. 165(1) and (2)).

(b) Measures consistent with R.4 appear to enable the confiscation of currency or BNIs.

The CC foresees that (1) Any objects used or intended to be used for the commission of an intentional offence or any objects obtained from such an offence shall be confiscated if they belong to the perpetrator at the time of the decision in the first instance. (2) The confiscation shall also include the replacement values of the objects designated in paragraph 1 which belong to the perpetrator at the time of the decision in the first instance. (3) No confiscation shall occur if such confiscation is disproportionate to the significance of the act or to the blameworthiness of the perpetrator (CC, Art. 19a).

Weighting and Conclusion

Liechtenstein adopted a disclosure system, and the Swiss Border Guard Corps carries out cash controls at the Liechtenstein border crossing posts to Austria. There is no declaration or disclosure system at the border between Switzerland and Liechtenstein. The disclosure system entitles the National Police to demand information on import, export, and transit of cash only if the amount of transferred cash is at least CHF 10 000 or the equivalent in a foreign currency, unless there is a suspicion of ML/TF. There is no provision to demand information on cash below CHF 10 000 in case of false disclosure or when information is withheld.

R.32 is rated LC.

Recommendation 33 – Statistics

In the 4th round MER of 2012, Liechtenstein was rated C with former R.32.

Criterion 33.1 - According to Art. 29a of the Law of 2 September 2020 amending the DDA (came into force in April 2021), the authorities shall, as a contribution to the preparation of the national risk analysis and for the purpose of reviewing the effectiveness of the national AML/CFT system, keep comprehensive statistics on the following elements relevant to the effectiveness of the system:

(a) (b) (d) - Number of SARs/STRs received and submitted to the FIU, measures taken as a result of these SARs/STRs - statistics on preliminary inquiries and investigations, including a number of persons indicted and convicted under section 165 of Liechtenstein's CC, indicating also the types of predicate offences and amounts of funds seized and confiscated. The same provision requires that statistics are kept with regard to the number of cross-border information requests made, received, refused, partially or fully responded by the FIU, broken down by requesting/requested state. (DDA Act, Art. 29a). Whilst the law does not require keeping statistics on MLA requests, the authorities advised that this statistics is kept by the Court and the Office of Justice, as required by a Decision of the Government of 2013 (LNR 2013-351), amended in 2021.

(c) Art. 29a of DDA Act requires keeping statistics on the value (in Swiss francs) of funds frozen and funds confiscated. It appears that there is no requirement that other types of property which is seized and/or confiscated need to be kept in the statistics database.

Weighting and Conclusion

Statistics is kept in line with the requirements of this Recommendation. The minor shortcoming concerns a lack of explicit requirements for keeping statistics on property other than funds which is seized and confiscated.

R.33 is rated LC.

Recommendation 34 – Guidance and feedback

Liechtenstein was rated LC with former R.25 in its 2014 MER. The existing guidance at the time did not address SAR/STR reporting, EDD, or CFT requirements.

Criterion 34.1 – Supervisory authorities must take necessary measures in the course of supervision, including issuing orders, guidelines, and recommendations (DDA, Art. 28 (1)(a)). Supervisory authorities are required to inform FIs and DNFBPs about their measures and procedures (DDA, Art. 28(2)) and they may issue guidelines interpreting the provisions of the DDA and the DDO as appropriate for each industry sector (DDA, Art. 28(3)).

The FMA issues: (i) business reports (annual reports on its activities, including licensing and supervision); (ii) guidelines; (iii) communications; (iv) instructions; and (v) recommendations (Rules on the Organisation of the FMA, 5.5 (internal)). The following are particularly notable: (i) FMA Guideline (2013/1) on the risk-based approach (revised 2021); (ii) FMA Guideline (2013/2) on inspections by mandated auditors and the FMA; (iii) FMA Communication (2015/7) on identification of BOs (revised 2018); (iv) FMA Communication (2017/3) on electronic reporting; (v) FMA Instruction (2018/7) which sets out sector specific interpretation of due diligence requirements (revised 2021); and (vi) FMA Instruction 2019/7 on safeguards applicable to relationships established on a remote basis.

Guidelines, communications, and instructions all appear to be issued under DDA, Art. 28(3) which refers to issuing "guidelines". The authorities have not explained the different uses for these different types of guideline. All are considered to be "enforceable means" by the authorities, taking account of criteria set in the FATF Methodology, based on jurisprudence set by the FMA Complaints Commission which hears first instance appeals against FMA decisions. In deciding on those appeals, the Commission has confirmed on several occasions that guidelines issued by the FMA are to be used as a "benchmark" for determining whether there have been violations of due

diligence obligations set out in the DDA and DDO. Failing to comply with guidelines is considered a failure to comply with underlying obligations.

The Chamber of Lawyers has issued the following publications: (i) business reports (annual reports on its activities); and (ii) Guideline for lawyers carrying out due diligence relevant activities. It also provides lawyers with newsletters - to raise awareness of the risks of ML/TF in the legal profession with practical examples.

Annually, "FMA practice" is published which gives information with regard to decisions and orders by the FMA, decisions of the FMA Complaints Commission as well as judgments of the Administrative Court and Constitutional Court in anonymous form.

The FMA also assists FIs and DNFBPs in applying AML/CFT measures through: (i) providing feedback to FIs and DNFBPs annually in relation to the latest inspection round in the context of a "Feedback Letter" (best practices and also compliance failings); (ii) regular and ad hoc meetings/ exchange of information/training events with professional bodies; (iii) management meetings with FIs and DNFBPs as part of ongoing supervision, including annual meetings for high risk entities (generally banks and TCSPs); (iv) training events for the private sector to assist in the application of the DDA/DDO; and (v) an annual workshop/conference for audit firms (feedback on latest inspection round and expectations for future inspections).

Similarly, the Chamber of Lawyers assists lawyers in applying AML/CFT measures by: (i) holding management meetings with supervised lawyers as required; and (ii) participating annually in training courses on the application of the DDA, which are organised by the University of Liechtenstein or the private sector.
The FIU has published a guidance paper titled "FIU Guidance" which explains the reporting requirements and the practical steps involved in submitting SARs/STRs to the FIU. In addition, since the introduction of the goAML reporting web portal, a goAML handbook has been directly distributed to all registered persons subject to the DDA and also published on the FIU's website. Common mistakes, general observations, methods, trends, typologies, and indicators for suspicion are also shared with the public through a specific section included in the FIU's annual report (published on its website). Furthermore, the FIU holds regular meetings with professional associations and individual FIs and DNFBPs covering reporting requirements, suspicions and how to deal with a reported business relationship after filing a SAR/STR. It has also published strategic analysis on VAs.

In relation to TF requirements, STIFA has published a factsheet for NPOs on TF risks (in German and English) (last updated in 2020) based on findings of the NPO Risk Report. This factsheet was jointly prepared with the FMA, FIU and the Fiscal Authority. The FIU has also published a Guideline on implementing the ISA.

The OPP participates every year in conferences addressed to FIs and DNFBPs and provides information about important decisions of the Court of Justice. The OPP has also issued guidelines for practitioners on pecuniary orders.

Weighting and Conclusion

R.34 is rated C

Recommendation 35 – Sanctions

Liechtenstein was rated LC with former R.17 in its 2014 MER. The report noted that administrative fines for institutions were not proportionate or dissuasive (at that time the maximum was CHF 100 000).

R.10 and R.22 lists activities to which the DDA does not apply and so which are not subject to regulation or supervision.

Criterion 35.1 – DDA/ Regulation (EU) 2015/847 - Non-compliance by individuals and legal persons with obligations under the DDA and Regulation (EU) 2015/847 (covered FIs and covered DNFBPs) are subject to: (i) criminal sanctions by the Princely Court of Justice (DDA, Art. 30); (ii) administrative sanctions by the supervisory authorities (DDA, Art. 31); or (iii) "supervisory measures". The limitation period for (i) and (ii) is three years, calculated from the point in time when the breach has ceased or been remedied. With the institution of legal proceedings, this limitation is set aside. Concerning individual cases of non-compliance detected during an inspection (e.g., in the case of a single customer), the limitation period might apply where the breach had already been remedied by the person subject to the DDA. However, if the individual case reveals more recent deficiencies within the AML/CFT system of that person, the FMA could initiate the necessary administrative sanctions.

The Princely Court of Justice may apply a custodial sentence of up to six months or a fine between two and 360 "daily units" for an offence on any person who wilfully: (i) violates reporting obligations; (ii) executes transactions in respect of which there is an obligation to make a report; (iii) fails to freeze assets subject to a TF report; or (iv) tips off. "Daily rates" are calculated by the courts based on the particular circumstances of the convicted person, with a minimum of CHF 10 and a maximum of CHF 1 000 (fines between CHF 20 and CHF 360 000). Even taking account of the possibility of punishing severe or repeated breaches with imprisonment of up to six months (and resultant criminal record), the range of sanctions available to the Court is not considered by the AT to be sufficiently proportionate given: (i) that it covers failure to report to the FIU (a key requirement of any AML/CFT regime); (ii) the higher range of administrative sanctions (fines) that may be applied for other failures to apply the DDA (by way of comparison – see c.27.4); and (iii) that it is not possible to imprison a legal person (which accounts for the majority of FIs and DNFBPs). The court may also impose fines for failing to provide information to the FIU, providing false information to the FIU or withholding significant facts from the FIU.

Criminal and administrative sanctions (fines) may only be imposed in the case of intent, otherwise (e.g., in the case of negligence) only supervisory measures (e.g., remediation orders) may be applied. Administrative sanctions and supervisory measures are considered under c.27.4 and 28.4(c)). Criminal and administrative sanctions (fines) require at least conditional intent as a subjective element i.e., there does not have to be deliberate intent. Based on jurisprudence (cases from the FMA Complaints Commission)[56], conditional intent is, in the case of administrative sanctions, very close to negligence (and not as narrow as it is in purely criminal proceedings). For conditional intention, a perpetrator does not need to realise the wrong; they do not even need to expect success. They need only to consider something possible.

The reduced maximum administrative sanction that may be applied to first offenders (see c.27.4 and c.28.4(c)) means that the range of sanctions in such a circumstance is not considered to be sufficiently proportionate.

TFS

[56] For example, FMA-BK 2017/15.

Wilful violation of TFS may be sanctioned by the Princely Court of Justice through a penalty of up to three years imprisonment or to a monetary penalty of up to 360 daily penalty units for (halved for negligent violation) (ISA, Art. 10). As explained above, "daily rates" are calculated by the courts based on the particular circumstances of the convicted person, with a minimum of CHF 10 and a maximum of CHF 1 000 (CHF 20 to CHF 360 000). Administrative penalties are considered under c.27.4.

NPOs

See c.8.4(b).

Criterion 35.2 – If violations are committed in the course of the business operations of a legal person, penalties may be applied to: (i) natural persons who are members of management, the board of directors, the supervisory board or in comparable functions (all referred to as the "executive body"); and (ii) any other natural persons who acted or should have acted on behalf of that legal person. In such a case, the legal person shall remain jointly and severally liable for financial penalties, fines, and costs (DDA, Art. 33(1)). Therefore, sanctions mentioned in Art. 30 and 31 DDA apply to directors and senior management.

Under c.27.4, it is explained that supervisory authorities may temporarily prohibit individuals from performing executive functions in the event of repeated, systematic, or serious violations of the DDA or Regulation (EU) 2015/847.

Weighting and Conclusion

The range of sanctions that may be applied by the Princely Court for failing to report to the FIU under the DDA or violating TFS is not considered to be sufficiently proportionate.

Shortcomings underlined under the conclusion to R.10 and R.22 with regard to the scope of application of the DDA (and consequently regulation and supervision) are also relevant here.

R.35 is rated PC.

Recommendation 36 – International instruments

In the IV round assessment Liechtenstein was rated LC with former R.35 and SR.I taking into consideration that some relevant articles of the Vienna, Palermo Conventions and also the TF Convention were not implemented.

Criterion 36.1 - Liechtenstein acceded to the Vienna Convention on 9 March 2007 and ratified the Palermo Convention on February 20, 2008 (as well as all three Protocols to the Palermo Convention since 20 February 2008 and December 2013: no reservation with regard to the Palermo Convention).

Liechtenstein also acceded the TF Convention on 9 July 2003 and the Merida Convention on 8 July 2010.

No reservations are in place with regard to these Conventions.

In addition to the above-mentioned conventions, Liechtenstein has ratified the Council of Europe Convention on Cybercrime (2001), to which it made specific reservations, on 27 January 2016. It entered into force on 1 May 2016.

Criterion 36.2 **-** Liechtenstein is a member of Europol and Interpol and is also a State party to the Council of Europe Convention on MLA in criminal matters.

Liechtenstein implements the conventions, including the Merida Convention, on the basis of the relevant provisions in national legislation and as follows:

The Vienna and Palermo Conventions are mainly implemented through the CPC, the Narcotic Act, and the MLA Act.

With regard to implementation of the Vienna Convention provision on confiscation, starting from July 2021, information gathering for seizure /confiscation purposes has been expanded thus allowing to gather information (e.g., information on financial relations and on BO) from all persons subject to the DDA – TT providers included (Art. 96 b (1) CPC as amended in July 2021). See also analysis under 31.1.

Since July 2019, tax savings are explicitly included in the definition of assets components for ML thus enlarging the scope of the ML offence and related implementation of these Convention.

The Terrorist Financing Convention is implemented in on the basis of the provision contained in the CC, CPC, the MLA Act, furthermore a set of provisions contained in the DDA supports TF Convention relevant provision implementation.

As regards the Merida Convention, implementation is ensured on the basis of the revised FIU Act, the DDA, the CC and CPC as well as on the basis of the MLA Act.

Implementation of the procedural side of the UNSCR 1267 and 1373 has been developed adequately and, based on the Terrorism Ordinance (June 2020), mechanisms for identifying targets for national designation were designed into the regulatory framework.

Weighting and Conclusion

Liechtenstein has ratified all the relevant Conventions and implements relevant articles.

R.36 is rated C.

Recommendation 37 - Mutual legal assistance

In the 4th round assessment, Liechtenstein was rated LC with former R.36 and SR.V taking into consideration that provisions under Art. 98a CPC did not allow for information gathering with some relevant categories, such as payment system providers, e-money institutions, insurance mediators, and DNFBPs.

Criterion 37.1 - Liechtenstein has a legal basis allowing authorities to provide rapidly a wide range of mutual legal assistance in relation to ML, associated predicate offences and FT investigations, prosecutions, and related proceedings, namely:

Mutual Legal Assistance Act of September 15, 2000 (MLA),

European Convention on Mutual Assistance in Criminal Matters (ECMA, ETS 30);

Second Additional Protocol to the European Convention on Mutual Assistance in Criminal Matters (ETS 182). The Protocol was ratified on 25 September 2020 and entered into force on 1 January 2021.

CoE Convention on Laundering, Search, Seizure and Confiscation of the Proceeds from Crime (Money Laundering Convention—MLC, ETS 141); and

Schengen Implementation Agreement December 19, 2011.

International cooperation regime is generally governed by the MLA Act and international conventions ratified by Liechtenstein. Based on Art. 1 MLA this Act applies unless otherwise provided for in international agreements.

Based on reciprocity, mutual legal assistance in criminal matters is granted according to Art. 1 and 3, paras. 1 and 50 MLA upon request of a foreign authority, including measures in relation to

matters of prevention, seizure and confiscation, as well as with regard to matters of redemption and criminal records, the proceedings for compensation of taking into custody and conviction, clemency cases and matters of sentence and measure (Art. 50 MLA). The CPC is applicable in all mutual legal assistance matters (Art. 9.1 MLA), unless otherwise provided in the MLA.

The range of assistance is broad and includes production, search, seizure of information, documents, or evidence (including financial records) from FIs, or other natural or legal persons, taking of evidence or statements, providing originals or copies of relevant documents and records, servicing judicial documents, facilitating the voluntary repatriation of assets and documents; identification, freezing, seizure, or forfeiture of assets laundered or intended to be laundered, the proceeds of ML and assets used for or intended to be used for FT, as well as the instrumentalities of such offences, and of assets of corresponding value.

Criterion 37.2 - The Office of Justice is the Central Authority in Liechtenstein for both MLA and extradition requests. Although there is no explicit reference to this in the legislation, the long-standing practice of having the Office as a central authority is also indicated in declarations made to some international conventions ratified by Liechtenstein (e.g., Council of Europe Convention on Laundering, Search, Seizure and Confiscation of the Proceeds from Crime).

Most of the incoming requests are processed through the Office of Justice or are directly addressed to the Court of Justice, particularly since the Schengen Agreement came into force in Liechtenstein. Only those requests that are not governed by the ECMA/Schengen Agreement or special bilateral treaties (e.g., Austria, Germany, Switzerland, or the U.S.) go through diplomatic channels.

All incoming requests are forwarded immediately to the Court of Justice by the Office of Justice, the former being a competent authority for execution of these requests (Art. 55, 57 MLA Act). On demand of the requesting authority, the Office of Justice is asking the Court of Justice for a status update and provides this information to the requesting authority.

All incoming requests are documented in a specific MLA database at the Office of Justice, for case management purpose.

Criterion 37.3 - The MLA process is subordinated to the general principle of reciprocity (Art. 3 MLA Act).

Grounds for refusal are provided on the basis of specific and mandatory grounds (Art. 51 MLA Act):

- the dual criminality requirement is not met (Art. 51 (1) (1) MLA Act);

- the request relates to a criminal offence which is not subject to extradition because of a political or military nature (Art. 51 (1) (1) MLA Act; Art. 14 and 15 (1) MLA Act; except if the criminal character outweighs the political motivation (Art. 14 no 2 MLA Act)[57];

- the request is based on proceedings that do not meet the basic principles of Art. 3 and 6 of the European Convention on Human Rights (ECHR; Art. 51 (1) (2) MLA Act; Art. 19 (1) and (2) MLA Act; e.g. torture);

[57] The fiscal nature of the offence is not a ground for refusal following amendment Law 2015 no 367 (see under 37 (4) (a)).

- the sentence or enforcement of preventive measures goes against the basic human rights (Art. 5 ECHR e.g., death penalty);

- the specific CPC conditions for confiscation or special investigative techniques (tapping, opening mail) have not been met (Art. 51 (1) (3) MLA Act); and

- the secrecy obligation cannot be lifted even by a Liechtenstein court decision (e.g., medical secret and lawyer's legal privilege; banking and other financial secrecy however does not fall under this category; Art. 51 (1) (3) MLA Act).

Refusals grounds are recognised as acceptable as a rule. While the formulation of Art. 51 MLA is strict and has a mandatory basis, it could in principle allows for some flexibility.

It has also been confirmed by the authorities that the political alibi cannot stop the requested assistance as soon as the offence is particularly serious, which would be the case of financing of terrorism or other terrorist related acts and authorities have informed that, since 2014 (last MER), no MLA cases were refused on the basis of political or military nature of the offence.

Criterion 37.4 - (a) MLA involving fiscal matters is regulated on the basis of the amendment of Art. 51 (1) (1) MLA Act (Law gazette 2015 no 367). Liechtenstein provides mutual legal assistance for a range of fiscal offences if dual criminality is met and if the circumstances of the case described in the MLA request of the foreign authority would be punishable by a court according to Liechtenstein's law, with imprisonment of up to six months.

Fiscal offences falling within this category that are punishable by a court in Liechtenstein are provided in (i) Art. 140 (tax Fraud) and 141 of the Tax Act (misappropriation of tax to be deducted at source); and (ii) Art. 88 (tax fraud), 89 (qualified tax evasion) and 90 (handling profits of tax evasion) of the VAT Act. Liechtenstein would therefore grant MLA with regard to these offences.

Provision of MLA for fiscal offences, based on the revised Art. 51 paragraphs 1, 3 and 4, is permitted even if otherwise specified in international agreements on international mutual legal assistance that entered into force before 1 January 2016 (Art. 51 (4) MLA Act).

b) Banking secrecy cannot prevent provision of MLA. Authorities advised that there is no need for lifting the bank secrecy by a court order given the provisions of Art. 96, 97, 97a, 98, and 98a CPC. In the context of MLA, it is of particular interest the disclosure obligations laid down by Art. 96b CPC (which, as of July 2021, replaced Art. 98a – Art. 98a had the same provision but it did not apply to all persons subject to the DDA). This article enables the investigative authorities to obtain relevant data and documents concerning a business relation, its nature, BOs behind it, and related transactions or operations from all persons subject to the DDA subject to due diligence. A specific issue on legal privilege (Art. 108 (2) CPC)) allows some persons to refuse to give testimony. It applies to defence counsels, lawyers, legal agents, patent lawyers and notaries on matters that have become known to them in their professional capacity. The authorities imposed measures to prevent abuse of this privilege (see R.31 – c.31.1).

Criterion 37.5 – The amended MLA Act (Art. 58e) regulates disclosure of confidential documents/information to the requesting country upon its substantiated request to obtain such documents/information. Entitled party(ies)' must be granted a hearing before the Court of Justice decides to render MLA, i.e., to render evidence gathered as per the request (Art. 55 para 4 MLA Act). Whilst the amended law does provide explicit provisions which require confidentiality of MLA requests and the information contained in them, the explanatory notes (report and motion No. 133/2020) discuss the matters related to C.37.5 and states that *confidential treatment of the request for MLA and the information it contains, as requested and justified by the requesting authority, <u>can</u> be taken into account. For reasons of investigative tactics, it is of great importance in certain investigative proceedings, especially at an early stage of the proceedings, that the*

persons concerned do not gain knowledge of the proceedings initiated against them or of individual procedural steps, especially since early knowledge can lead to the thwarting of the investigation or any further investigative steps, especially against any possible accomplices. The amended Act (Art. 58e) now provides that the Court of Justice may issue a prohibition order (prohibition of disclosure) to the person subject to the DDA from whom documents/information were requested. This prohibition means that they must not inform anyone (including suspects) of the procedure and information/documents requested from them by the competent authorities. This prohibition may last for a period of 24 months. The Act now also provides for the possibility to transmit the relevant objects, documents, and data to the requesting authority whilst the 'entitled party' would be heard before the court only after the prohibition of disclosure has been lifted. In addition, the Court of Justice may grant confidential treatment of the request for MLA and the information contained therein if the following conditions are fulfilled: (i) confidential treatment of the request for MLA and the information it contains is requested and justified by the requesting authority and if, due to the specific features of the case, (ii) all prerequisites of Art. 58e MLA Act are met. Consequently, confidentiality of MLA requests is optional and depends on specific features of the case.

Criterion 37.6 - If the requesting state is party of the European Convention on Mutual Assistance in Criminal Matters (ECMA) dual criminality is not a condition if no coercive measures are involved (Art. 1 and 5 ECMA).

If the requesting state is not party of the European Convention on Mutual Assistance in Criminal Matters (ECMA) dual criminality is a condition for rendering assistance (Art. 51 (1) MLAA); there are exceptions in bilateral treaties (in particular with Austria and with the United States).

Lastly, pursuant to Art. 51 (2) MLA Act the fact that an action is not liable to prosecution under Liechtenstein law is not an obstacle for provision of documents if the addressee is willing to accept them.

Criterion 37.7 - Where dual criminality is required, it is sufficient that the conduct underlying the offence is criminalised in both Liechtenstein and the requesting country (Art. 51 (1) (1) MLA Act); Authorities also advised that the case law confirmed the application of this principle in practice.

Criterion 37.8 - All investigative powers available to the Liechtenstein law enforcement and other competent authorities are also available in MLA proceedings (Art. 9 (1) MLA Act).

(a) With regard to the powers of law enforcement authorities such as production, seizing and obtaining of documents, Art. 96b CPC enables authorities to obtain relevant data and documents concerning business relation, its nature, BOs behind it, and related transactions or operations. This provision is applicable to all entities (persons) subject to due diligence.

(b) Pursuant to Art. 9 (1) MLA Act, the CPC and investigative techniques available at the national level apply mutatis mutandis unless otherwise provided for in this Act. All relevant investigative techniques are available in MLA proceedings.

Weighting and Conclusion

Technical shortcomings in relation to this Recommendation include some limitations with regard to the possibility(ies) to maintain confidentiality of MLA requests and to the capability to provide assistance in absence of dual criminality, where no coercive actions are requested. The latter, however, has almost no effect given the origin of the requests received by Liechtenstein authorities (vast majority are covered either through ECMA and bilateral treaties) and thus the AT did not give noteworthy weighting to this shortcoming.

R.37 is rated LC.

Recommendation 38 – Mutual legal assistance: freezing and confiscation

In the 4th round MER, MLA on confiscation and freezing was not under the scope of evaluation. Given that this Recommendation was rated LC in the 3rd round of MER in 2008. Deficiencies identified included restricted confiscation for instrumentalities in MLA context and the fact that Liechtenstein did not take an asset forfeiture fund into serious consideration.

Criterion 38.1 – All investigative powers of Liechtenstein's law enforcement authorities are also available in MLA proceedings (Art. 9 (1) MLA Act; see c.4.1 and c.4.2.). Liechtenstein is able to grant MLA to requests by foreign countries to identify, freeze, seize, confiscate or forfeit assets if the circumstances of the case described in the MLA request of the foreign authority would result in forfeiture, extended forfeiture, confiscation or a deprivation order according to Liechtenstein law. As noted under R.4, all elements discussed under points (a) to (b) are covered for MLA purposes.

Criterion 38.2 – The MLA Act also applies to civil forfeiture proceedings (Art. 50 (1a)). The Court of Justice has the authority to take expeditious action in response to requests by foreign countries to identify, freeze, seize or confiscate the laundered property, proceeds from and instrumentalities used (or intended for use) in ML, TF and predicate offences or property of corresponding value. Art. 64 (1) MLA Act provides the legal basis for the execution of foreign court decisions, especially in connection with pecuniary orders. Pursuant to Art. 50 (1a) MLA Act foreign civil proceedings for the pronouncing of a pecuniary order within the meaning of Art. 20 and 20b CC (non-conviction-based proceedings) are deemed a criminal matter for the purpose of Art. 50 (1) MLA Act. Thus, legal assistance can be granted also in non-conviction-based proceedings.

Criterion 38.3 – a) Authorities advised that, despite the fact that Liechtenstein has no formal arrangements for co-ordinating seizure and confiscation actions with other countries, the country provides assistance and coordinates seizure and confiscation actions through CARIN and Eurojust networks. To confirm that seizure of assets is executed upon foreign authorities' request(s), Liechtenstein provided a case where a funds of a foreign former politician were frozen by Liechtenstein courts based on MLA requests submitted by two countries. In addition, freezing of assets and seizing of instrumentalities in a domestic case, according to the established case law, does not inhibit imposing similar measures on the same assets or instrumentalities based on an MLA request in the course of MLA related proceedings. This has been confirmed by the Constitutional Court in its decision dated February 6th, 2006 (StGH 2005/45; LJZ 2007, 338). The decision states that it is not contrary to Art. 64 (4) MLA Act if a freezing order is imposed on the same funds/assets in both - domestic criminal proceedings and mutual legal assistance proceedings.

b) Freezing and seizure takes the assets and items into judicial custody (Art. 96 and 97a CPC – see also R.4). Frozen assets usually stay at the bank accounts. Once there is a confiscation or forfeiture decision from the court, objects or assets, which have been seized or frozen will become property of the state. In case of an enforcement of a foreign pecuniary order, forfeited assets and objects subject to confiscation or to a deprivation order also devolve upon the state (Art. 64 (7) MLA Act).

Criterion 38.4 – In the case of offences committed abroad, the government may, pursuant to Art. 253a CPC, conclude an agreement with the state where the offence was committed with respect to the sharing of forfeited or deprived assets and may, in particular, include conditions in such agreement concerning the use of such assets.

Weighting and Conclusion

R.38 is C.

Recommendation 39 – Extradition

In the 4th round MER of 2014, extradition was rated C. Still the authorities were recommended to adopt legislation introducing serious tax crimes as extradition ground and at a minimum expand the possibility to extradite for serious VAT fraud beyond the Schengen area.

Criterion 39.1 – The general extradition rules are laid down in Chapter II of the MLA Act (Art. 10 to 49 and Art. 68 to 70). These rules are applied if international conventions do not stipulate otherwise (Art. 1 MLA Act). Pursuant to Art. 11 (1) of the MLA Act, extradition for prosecution is permissible for acts committed wilfully which are sanctioned, under the law of the State making the request, with imprisonment of more than one year or with a preventive measure of the same duration, and, under Liechtenstein law, with imprisonment of more than one year. Extradition for enforcement of sanction pursuant to Art. 11 (2) of the MLA Act is permissible if imprisonment or the preventive measure has been pronounced due to one or more of the offences mentioned in para 1 of Art. 11 (see above) and if at least four months imprisonment are still to be enforced. If the requesting state is a member of the Council of Europe, the extradition regime between Liechtenstein and the requesting state is governed by the European Convention on Extradition (ECE).

a) Both ML and TF are extraditable offences under Liechtenstein law (Art. 11 (1) of the MLA Act). Extradition proceedings can be initiated in two different ways. Either through execution of an international arrest warrant by police or through request of a foreign authority for extradition which leads to a provisional arrest. In both cases it is required that a formal extradition request is submitted together with a valid arrest warrant including the relevant facts and the applicable penal provisions. If the conditions for arrest are met, then it is executed either by international warrant or by court order. The detainee is presented to the examining judge for questioning. After the interrogation, decision will be taken whether the detention is to be ordered. If the detention is ordered and as soon as the necessary documents have been provided by the requesting authority, the file will be submitted to the Court of Appeal to examine the admissibility of the extradition. If admissibility is confirmed, the file will be sent to the Office for Justice. The Minister of Justice will order the surrender of the person to be extradited when the requirements according to Art. 32 MLA Act are met. Details for coordinating the extradition are communicated directly between the police authorities. Although there are no formal prioritisation criteria in place, particular attention is given to the requests for arrest and extradition. According to Art. 29 (4) MLA Act preventive detention prior to an extradition may only last for six months. Extradition cases need to be finalised within this period.

b) The database regarding extradition allows the Office of Justice (which is also in charge to keep and update this database) to monitor a case. It also allows to produce statistics and to find open cases and connected cases. In Liechtenstein, extradition cases mostly concern the situations where the person(s) subject to request(s) are in custody and consequently they are always dealt with on an expedited basis.

c) There are no provisions which place unreasonable or unduly restrictive conditions on the execution of requests (see Art. 14 to 21 of the MLA Act).

Criterion 39.2 – a) A Liechtenstein national pursuant to Art. 12 of the MLA Act can only be extradited to another State or surrendered for prosecution or enforcement of a sentence if he/she, after having been informed about the consequences of his/her statement, has given his/her explicit consent. This must be laid down in the court record. The person can revoke his/her consent up to the time when the surrender has been ordered.

b) If a Liechtenstein national is not extradited at the request of foreign authorities, pursuant to Art. 6 (2) of the European Convention on Extradition (ECE), the country is obliged to submit the

case to the OPP as the national competent authority in order that proceedings may be taken if they are considered appropriate.

Irrespective of the applicability of Art. 6(2) ECE and of a request for the assumption of prosecution, the Ministry of Justice and the courts as the competent national authorities for extradition, are obliged to submit the request of the country seeking extradition of a Liechtenstein national and the facts of the case to the OPP for the purpose of initiating an investigation of the offences set forth in the request (Art. 53 and 54 CPC).

The Office of the Public Prosecutor is ultimately responsible for the investigation and the prosecution of all offences, including ML, associated predicate offences and TF , in accordance with Art. 20 to 22 CPC. If Liechtenstein does not extradite a national, the OPP – even without a request for the assumption of prosecution – is obliged to initiate an investigation because Liechtenstein criminal legislation also applies to criminal acts committed abroad under the conditions set forth in Art. 64 and 65 CC.

Criterion 39.3 – Where dual criminality is required it is sufficient that the conduct underlying the offence is criminalised in both Liechtenstein and the requesting country (Art. 11 MLA Act.

The Liechtenstein Supreme Court ruled in a decision dated October 1st, 2008 (11 RS.2006.192-37; LJZ 2009, 142) that a different legal qualification of the facts by the requesting state does not inhibit a procedure and understanding of an application of dual criminality in Liechtenstein – and that is that dual criminality principle is satisfied even if both countries (requesting and requested) do not place the offence within the same category or the same legal definition, provided that the both countries criminalise the conduct underlying the offence.

Criterion 39.4 – Simplified extradition is possible under Art. 32 of the MLA Act, if the person to be extradited due to a foreign request for extradition, has consented to his/her extradition during his/her questioning and agreed to be surrendered without carrying through the formal extradition proceedings (MLA Act, Art. 32 (1)). If consent to simplified extradition has been given, no formal extradition request is required (MLA Act, Art. 32 (1a)).

Weighting and Conclusion

R.39 is rated C.

Recommendation 40 – Other forms of international cooperation

In the 4th round MER, Liechtenstein was rated PC with regard to R40.

Main deficiencies were related to shortcomings affecting the DDA and the FIU Act that were in force at that time, mainly with regard to secrecy provisions of the DDA preventing information exchange with foreign authorities and issues concerning the FIU access to information held by obliged subjects that also affect the FIU capability to share information.

Technical deficiencies identified in the 4th round have been addressed by the Liechtenstein authorities in the course of the follow-up process to a level equivalent to LC.

Criterion 40.1 –

Police- The National Police are able to share both spontaneously and upon request, information on the basis of Art. 35 of the Police Act. A trilateral police cooperation agreement is in place with Austria and Switzerland. In addition, other information exchange channels such as INTERPOL (via the National Police) and liaison officer network are used to exchange information in relation to ML, predicate offences, and TF.

FMA- The FMA can exchange information with competent foreign authorities in other EEA Member States for the purpose of performing their supervisory duties (Art. 26b FMA Act). Same

provision applies with regard to cooperation with authorities of third countries, insofar as the provisions of Regulation (EU) 2016/679 have to be complied with (in particular Art. 44 et seq. of the GDPR).

Liechtenstein also exchanges supervisory information related to subsidiaries and branches of Liechtenstein FIs or foreign subsidiaries represented in the country in the course of bilateral meetings with foreign supervisors (Switzerland, Austria, Singapore, Hong Kong).

The exchange of information provided to the FMA by the Chamber of Lawyers is subject to the consent of the Chamber of Lawyers as "data-owner". Generally, the FMA obtains consent from any national authority prior to transmitting information obtained from said authority.

As per the legislation specifically covering AML/CFT related cooperation, starting from April 2021, the revised text of Art. 37 DDA empowers all supervisory authorities to exchange all information, as well as personal data concerning criminal convictions and offences, to foreign supervisors that perform equivalent tasks. The provision is applicable for cooperation with both EEA countries as well as third countries. Information exchange is made upon request and spontaneously. According to Art. 37 DDA, information can be shared with supervisory authorities having tasks in the field of combatting ML, organized crime or TF, while there is no direct power to exchange information on predicate offences. While the legislative merits of cooperation assigned to the FMA are not generally wide, these types of information would generally be exchanged via other competent authorities, i.e., the FIU and LEAs.

FIU- On the basis of the revised (2016) FIU Act (FIUG), the FIU can provide information and / or pass on documents to foreign FIU concerning the detection of ML, predicate offences, organised crime and the financing of terrorism.

Fiscal Authority- The Fiscal Authority is responsible for exchange of information with foreign tax authorities on the basis of agreements concluded in the field of taxation since 2009. Liechtenstein introduced the AEOI in 2016 and the FATCA agreement with the United States was signed in 2014. Customs cooperation is based on the customs and monetary union agreement with Switzerland.

Criterion 40.2 –

(a) Competent authorities have a lawful basis for providing international co-operation (see 40.1).

(b) Nothing hinders competent authorities' capability to use the most efficient means to cooperate.

(c) FIU uses Egmont secure Web. The National Police uses Interpol channels (e.g. Global Focal Point Platform on Asset Recovery) /Europol (e.g. SIENA-CT, SIENA-ACA), CARIN-network, Liaison Officer network, SecEMAIL-System, special channels (encrypted mail) with Intelligence Services.

The FMA uses special encrypted communication channels with the European Supervisory Authorities - EBA, ESMA and EIOPA. When exchanging information with foreign supervisory authorities the FMA uses encrypted e-mails or offers a secure cloud storage application (SecureSafe) where foreign competent authorities can download the requested information/data.

(d) Authorities have set internal process to deal with requests. Apart from the FIU, operational authorities in Liechtenstein do not receive/sent an exceeding number of such requests per year. Consequently, a prioritization issue does not come up at all and timely execution is granted as a standard.

Generally, the FIU receives approximately 1 request per workday and response is feasible timely. In case of urgency the FIU applies its best efforts to execute it mindful of the type and nature of the request.

(e) All competent authorities possess secured IT systems, and their employees are subject to official secrecy. In addition, Art. 4 of the Ordinance on Personnel Security Checks (PSPV) stipulates that all state personnel handling confidential information are subject to personal security checks carried out by the National Police. The National Police has issued a set of instructions on IT systems (DA IT-Resources) that applies to all employees. Its purpose is to ensure trouble-free operation and to guarantee information security and data protection. In addition, the National Police has compiled information on data protection for all employees on an information sheet.

Within the FMA information security is in the responsibility of the Executive Board and an employee has been appointed as respective officer (as well as a deputy) for those tasks. In order to safeguard information received – which includes information from competent foreign authorities- within the FMA, the FMA implemented various internal measures such as a comprehensive information security management system (ISO 27001), GDPR-compliant data protection measures, electronic data management system (DMS) where all information is recorded/saved, "clean desk policy", "clean screen policy" and issuance of Guidance for security purposes. The FMA uses special encrypted communication channels with the European Supervisory Authorities - EBA, ESMA and EIOPA. When exchanging information with foreign supervisory authorities the FMA uses encrypted e-mails or offers a secure cloud storage application (SecureSafe) where foreign competent authorities can download the requested information/data. With some counterparts, the regular postal service is still being used.

Criterion 40.3 –

FIU- In principle, the FIU does not require MoUs with Egmont Group member counterparts in order to exchange information. However, Art. 7(4) FIU Act allows the FIU to enter such agreements, after consulting the competent member of the Government (see also R.29).

FMA- The FMA does not need bilateral or multilateral agreements for information exchange purposes. The general principle contained in Art. 37(8) DDA applies on which basis the supervisory authorities may conclude agreements with the competent foreign supervisory authorities on practical arrangements for the exchange of information. In addition, Art. 41g and 30q (1) of Banking Act (BankG) provides that cooperation agreements are put in place between the FMA and the other competent authorities of the EEA Member States/ third countries in order to facilitate effective supervision. In the field of insurance supervision, the FMA may conclude agreements with foreign supervisory authorities (Art. 188 (2) Law on the Supervision of Insurance Undertakings; VersAG).To date, the FMA has signed 13 MoUs. The amended Art. 37 (8) DDA stipulates that the supervisory authorities may conclude agreements with the competent foreign supervisory authorities on the practical arrangements for the exchange of information.

Police- The National Police does not require a bilateral or multilateral agreement to co-operate with its counterparts (Art. 35 et seq.). Cooperation is conducted on the basis of reciprocity. A Trilateral Police Cooperation Agreement is in place between Liechtenstein, Switzerland and Austria.

Fiscal Authority- The Fiscal Authority is in charge for the international co-operation regarding EOIR (exchange of information on request for tax purposes), SEOI (spontaneous exchange of information in tax matters) as well as AEOI (automatic exchange of information in tax matters). The international co-operation in tax matters is based on the different relevant international

agreements, such as the multilateral competent authority agreement (MCAA-CRS) or the AEOI Agreement Liechtenstein-EU[58].

Criterion 40.4

There are no specific legal provisions regulating explicitly the provision of feedback to the authority from which assistance was sought and providing this in a timely manner. However, there are no provisions which would pose an obstacle to doing so.
Given its Egmont Group membership, the feedback on the use of data and outcomes of the analysis is provided by the FIU to the foreign authority spontaneously or upon request (in line with the Clause 19 of the Egmont Group Principles). There is no indication that this should be done in a "timely manner".
The FIU may also physically visit counterpart FIUs aimed at discussing common trends, methods, typologies and risks.

FMA confirms receipt of the information provided by foreign authorities and acknowledges its usefulness. Where information received is inaccurate or insufficient the FMA follows up by means of direct contact in order to amend the original request. Some feedback is also given during bilateral meetings with other supervisory authorities (such as with for e.g., FINMA, BaFin, MAS with which regular meetings take place).

The National Police does not have a standard procedure for giving feedback to foreign authority which has provided information, but it may give feedback depending on the situation, notably if the information provided is incomplete.

Criterion 40.5

Competent authorities do not prohibit or place unreasonable or unduly restrictive conditions on the provision of information or assistance. Applicable laws do not provide for the possibility to refuse cooperation based on the grounds provided under c.40.5 of the Methodology.

As regards the cooperation provided by the FMA, Art. 37 (1) and (2) of the DDA allows for information exchange provided that, the exchange is not detrimental to sovereignty, security and public order or other significant national interest. National interest is understood of severe gravity and, according to Authorities, this caveat has never been applied. Requests may not be refused in cases where tax issues are involved.

The FIU Act (Art. 7) allows the FIU to submit financial, administrative and law enforcement information to foreign FIUs, on the basis of reciprocity, provided the information will be used exclusively for analysis purposes in the prevention of ML, predicate offences to ML, organised crime and TF. It should also be ensured that the information passed on will only be communicated to third parties with the consent of the FIU and the requesting FIU is subject to official secrecy. The fact that the request involves a tax issue does not constitute ground for refusal for the FIU.

As regards the National Police, Art. 35 of the Police Act) sets the basic principle of the international administrative assistance, where administrative assistance would be refused in very limited circumstances. Although cooperation is refused if the fact is related to taxes issues,

[58] List of all Double Taxation Agreements (DTA) and Tax Agreements regarding Exchange of information available at:

https://www.llv.li/inhalt/11469/amtsstellen/internationale-steuerabkommen

the authorities claim that this is mitigated by the fact that where a misdemeanour under article 140 (tax fraud) of the Tax Act or under articles 88 (tax fraud) or 89 (qualified tax evasion) of the Value Added Tax Act is a predicate offence for ML, administrative assistance is granted. The extent to which it would be granted in practice is unclear.

The Fiscal Authority is the competent authority regarding exchange of information (EOI) in tax matters which is based on international agreements. Information provided may be used for the determination, assessment, enforcement or collection of taxes as well as for the investigation and prosecution of criminal tax matters. Liechtenstein is able to provide information in various forms, including on request, spontaneously as well as on automatic basis. Liechtenstein is a member of the Global Forum on Transparency and Exchange of Information for Tax Purposes as well as the BEPS Inclusive Framework and therefore subject to continuous peer review procedures which throughout confirm high conformity and effectiveness of the tax transparency measures of Liechtenstein.

Criteria 40.6 - The DDA Art. 37 1(c) explicitly requests that information and data are provided on the basis that transmitted information will be used only for the purposes referred on the basis of the Act (performing of the duties of the requested foreign authority based on the DDA or on the respective requesting authority framework in the field of combating ML /TF) . In case of information originating from abroad, the exchange is allowed on the basis of express consent from the authority which transmitted the information, and it is ensured that the information is disclosed only for the purposes for which that authority expressed consent (Art. 37 (1) d DDA).

Information exchange by the FIU is allowed on the basis that the information will be used exclusively for analysis purposes in the prevention of ML, predicate offences to ML, organised crime and TF (Art. 7 FIU Act). As an Egmont member, the GFIU applies the Data Protection and Confidentiality of Egmont's Principles of Information Exchange.

As regards the National Police, according to Art. 35 of the Police Act personal data transmitted to foreign security authorities or organisations may be used for purposes other than those on which the transmission is based only with the prior consent of the National Police. No such requirement is specified in the law for incoming information.

Tax information is protected on the basis of Art. 38 Personnel Act. (Official secrecy).

Criterion 40.7 – The same level of confidentiality is kept for information exchanged and for requests received on the basis of Art. 38 Personnel Act**.** Basically, no distinction exists between the level of protection of information from foreign authorities and domestic sources.

The transfer of personal data to a competent supervisory authority in a third country is only permitted if the conditions laid down in Chapter V of Regulation (EU) 2016/679 are met (Art. 37 (9) DDA and also Art. 26b (3) FMA Act). There is, however, no express provision allowing authorities to refuse to provide information if the requesting authority cannot protect information effectively.

The FIU's obligations in relation to maintaining appropriate confidentiality for any request for co-operation and the information exchanged, consistent with both parties' obligations concerning privacy and data protection are provided under the FIU Act in compliance with the Egmont Group Principles.

As per the National Police, the latter would be able to reject cooperation if appropriate guarantees pursuant to Art. 78 of the Data Protection Act for adequate data protection would not be ensured, subject to Art. 79 of the Data Protection Act.

Criteria 40.8 - Competent authorities can conduct inquiries on behalf of their foreign counterparts and exchange all information that would be obtainable by them if such inquiries were being carried out domestically.

On the basis of the revised text of Art 37(5) DDA co-operation with competent foreign supervisory authorities has been expanded to the greatest possible extent since it also includes conducting investigations within the powers of the competent authority whose assistance has been requested, on behalf of the requesting competent authority, and the subsequent exchange of information obtained in the course of such investigations.

The FIU is empowered to provide administrative, financial and law enforcement information to foreign FIUs and the relevant provision (Art. 7 FIU Act) does not limit the FIU capability to obtain information it would have obtained for domestic inquires.

Art. 35a Police Act provides the legal basis for the administrative assistance by the National Police and does not limit Police capability in case of foreign counterparts' requests. As for the Fiscal Authority, with the implementation of international standards regarding exchange of information in tax matters (including on request, spontaneously, and automatically) the Fiscal Authority is in the position to gather and provide information to its foreign counterparts that is foreseeably relevant for the administration or enforcement of their domestic tax laws (see for example Art. 4 of the Multilateral Convention (MAC)). For that purpose, the international tax treaties as well as the domestic laws implementing those tax treaties provide that the Fiscal Authority uses it information gathering measures in order to have access to the relevant information, even though Liechtenstein might not need such information for its own tax purposes.

Criterion 40.9 - The FIU may, while performing its duties, request foreign FIUs to provide information or pass on documents if required for the purposes of the FIU Act (FIU Act, Art. 7 (1)).

The FIU is permitted to pass official information that is not accessible to the public to foreign FIUs, if: a) this does not compromise sovereignty, security, public order or other essential national interest; b) it is guaranteed that the requesting FIU would comply with a similar request from Liechtenstein; c) it is guaranteed that the information passed on will be used exclusively for analysis purposes in the prevention of ML, predicate offences to ML, organised crime and TF; d) it is guaranteed that the information passed on will only be communicated to third parties with the consent of the FIU; e) the requesting FIU is subject to official secrecy (FIU Act, Art. 7 (1)).

Criterion 40.10 - There are no barriers for FIU to provide feedback to foreign FIUs. Authorities advise that the FIU provides feedback to foreign counterparts in accordance with the Egmont Group Principles for Information Exchange.

Criterion 40.11 - (a) No provision in the law hinder the FIU's ability to exchange information. At the same time, no barriers are stipulated by the law which would undermine the scope of information to be exchanged as formulated under this criterion.

(b) Scope of information subject to exchange is not specified by the law. Given that no barriers which would undermine the scope of information to be exchanged are present in the legislation means that the requirements of this criterion are met.

Criterion 40.12 - The FMA can provide cooperation to a similar supervisory authority outside of Liechtenstein (FMA Act, Art. 26b). This is permitted for AML/CFT purposes with supervisors in EEA Member States as well as with third Countries (DDA, Art. 37). While the sectoral laws provide for cooperation within that sectoral subject matter, cooperation for AML/CFT purposes is primarily governed by the DDA.

The FMA may share all necessary information, reports, documents, data, and personal data, including personal data concerning criminal convictions and offences, to competent foreign

authorities in other EEA Member States, insofar as this is necessary for the performance of their supervisory duties (FMA, Act, Art. 26b).

This provision also allows the FMA to cooperate with competent authorities in third (non-EEA) countries, insofar as the provisions of data protection legislation, in particular Art. 44 et seq. of Regulation (EU) 2016/679, are complied with.

The FMA is empowered to enter into agreements with competent foreign authorities for the purposes of cooperation (FMA Act, Art. 26b (4)), although this is not a prerequisite for cooperation to occur.

Exchange of information provided to the FMA by the Chamber of Lawyers is subject to the consent of the Chamber of Lawyers as "data-owner" and the FMA generally obtains consent from any national authority prior to transmitting information obtained from the said authority.

Criterion 40.13 –

As provided at c.40.12, the FMA, Act, Art. 26b/DDA, Art. 37 allow for all domestically available information to be shared with foreign counterparts.

Criterion 40.14 –

As provided at c.40.12, the FMA, Act, Art. 26b/DDA, Art. 37 allow for the exchange of regulatory, prudential or AML/CFT information - when relevant for AML/CFT purposes - with foreign counterparts.

In addition, regulatory and prudential information can also be exchanged pursuant to the applicable sectoral law(s). In addition to the information that can be exchanged under c.40.12, the FMA shall grant the authority responsible for exercising group supervision access to any information relevant for the purpose of that supervision.

Criterion 40.15 – Supervisory authorities can request all information (including BO information) from persons subject to the DDA that they require to perform their oversight functions under the DDA (DDA, Art. 28 (4)). These oversight functions include the power to co-operate with foreign supervisory authorities (DDA, Art. 37).

In addition, supervisory authorities must cooperate with competent foreign supervisory authorities to the greatest extent possible in the supervision of FIs (DDA, Art. 37 (5). Such cooperation may include conducting investigations within the powers of the competent authority whose assistance has been requested, on behalf of the requesting competent authority, and the subsequent exchange of information obtained in the course of such investigations.

Competent financial market supervisors of an EEA Home State also have the option of carrying out inspections in Liechtenstein in the premises of their branches, subsidiaries etc. The supervisory authority of the EEA Home State must coordinate such an inspection with the FMA beforehand. As of 1 April 2021, this also applies to non-EEA supervisors (DDA, Art. 37 (7)).

Criterion 40.16 – Supervisory authorities may request information from foreign supervisory authorities (including personal data concerning criminal convictions and offences), necessary for the performance of duties imposed by the DDA (DDA, Art. 37 (3)). Supervisory authorities may share such information with domestic authorities for specified purposes (without prior authorisation from the requested authority), namely: (i) to exercise obligations with regard to the prevention of ML, organised crime, and TF or other national or European regulations as well as regarding prudential supervision, including impositions of penal and administrative measures; (ii) for the conduct of proceedings regarding legal remedies against a decision of the supervisory authorities, including court proceedings connected thereto; and (iii) for the conduct of court proceedings pursuant to EU Directive 2015/849 (DDA, Art. 37 (4)).

There is no requirement on the FMA to inform a foreign supervisor that it (FMA) is obliged to share information domestically (or that it is, in fact, sharing that information), although the FMA does so as a matter of good practice.

Further, the FMA may share all information originating from abroad with foreign supervisors, provided express consent has been given by the originating authority and provided that the information will only be disclosed for the purposes to which these authorities have consented (DDA, Art. 37 (1) (d)).

Criterion 40.17 - From the legislation provided to the AT, it appears that Liechtenstein has appropriate basis to cooperate only with the EU Member States and those signatories of the CoE Convention on MLA. In summary, the authorities advise that the legal basis for international co-operation is the Trilateral Police Cooperation Agreement and Art. 35ff. of the Police Act as well as international conventions ratified by Liechtenstein (i.e., the European Convention on Mutual Assistance in Criminal Matters and its Second Additional Protocol and the CoE MLA Convention).

In line with the Police Act, Art. 35(f)), the National Police shall provide the competent law enforcement authorities of the other EU/Schengen countries with information a) on request, to the extent that such information is necessary to conduct a criminal investigation or a criminal intelligence operation; b) without any prior request, to the extent that such information may be relevant for the prevention and prosecution of the serious criminal offences, including ML and TF. The scope of information subject to exchange includes any type of data held by the National Police, except data gathered through the use of coercive means or for gathering of which a use of coercive means is necessary (Police Act, Art. 35 (e)). Exchange of information between the National Police and law enforcement authorities of the other EU/Schengen countries shall take place through the channels available for international law enforcement cooperation. (Police Act, Art. 35(g)). Authorities advise that according to Art. 4 Agreement on Operational and Strategic Co-operation between the Liechtenstein and Europol, the co-operation may, in addition to the exchange of information and in accordance with the tasks of Europol as outlined in the Europol Council Decision, include the exchange of specialists' knowledge, general situation report, results of strategic analysis, information on criminal investigation procedures, information on crime prevention methods, participation in training activities as well as providing advice and support in individual criminal investigations.

As regards cooperation with non-EU member states, while the Police Act does not restrict the cooperation, Art. 35h provides that stricter rules for the disclosure of information may be applied in relation to foreign law enforcement authorities than to domestic law enforcement authorities. Nonetheless, they shall not apply to law enforcement authorities of the EU/Schengen countries. Thus, the law provides for the possibility of limited cooperation with non-EU members.

Criterion 40.18 – Upon request of foreign counterparts the National Police can use its powers to conduct inquiries (including any investigative techniques available) and obtain information (except coercive measures which only can be ordered by the court). Pursuant to Art. 35a (1) of the Police Act the National Police can provide administrative assistance by (among others) granting and supporting foreign undercover investigations on Liechtenstein territory and carrying out other measures which do not require a court order. This includes the situations as follows: a) upon request, provided that doing so is necessary for foreign security authorities or organisations to perform their duties and provided that there is reciprocity; b) on its own initiative, where this could be relevant in a specific case for the recipient to assist in averting specific dangers to public safety and order or to prevent and combat criminal offences (Police Act, Art. 35(2)).

The National Police may provide administrative assistance by a) transmitting personal data, including special categories of personal data, such as in particular genetic data, biometric data uniquely identifying a natural person, and health data, and personal data relating to criminal

convictions and offences, as well as data based on profiling; b) granting and supporting foreign undercover investigations on Liechtenstein territory; c) carrying out other measures which do not require a court order. (Police Act, Art. 35a (1)).

Cooperation with Europol is elaborated under C.40.17.

Criterion 40.19 - The National Police may establish or participate in joint investigation teams with competent authorities of other jurisdictions for the investigation of any criminal offence including ML, associated predicate offences and FT. The relevant legal basis is Art. 35a(1b) of the Police Act providing administrative assistance by granting and supporting foreign undercover investigations on Liechtenstein territory.

The trilateral Cooperation treaty with Switzerland and Austria also includes provisions about the cross-border surveillance, the cross-border pursuit and the controlled delivery. This agreement allows to build joint surveillance/investigation teams. Furthermore, the Second Additional Protocol to the European Convention on Mutual Assistance in Criminal Matters that has been ratified by Liechtenstein on 25 September 2020 provides the States Parties with the possibility to set up joint investigation teams (Art. 20).

Exchange of information between non-counterparts (40.20)

Criterion 40.20 - No specific rules or regulations that would prohibit competent authorities to exchange information indirectly with non-counterparts are in place in Liechtenstein.

Weighting and Conclusion

Liechtenstein has a sound legal basis for cooperation by different state authorities. There is no requirement on the FMA to inform a foreign supervisor that it (FMA) is obliged to share information domestically, although the FMA does so as a matter of good practice. Stricter rules apply on cooperation of the National Police with non-EU members.

R.40 is rated LC

Summary of Technical Compliance – Deficiencies

ANNEX TABLE 1. COMPLIANCE WITH FATF RECOMMENDATIONS

Recommendations	Rating	Factor(s) underlying the rating
1. Assessing risks & applying a risk-based approach	**LC**	• Especially for the VASP sector, final residual risk levels in NRA II appear to reflect more expected capability of the regulatory framework to mitigate risks than actual level of application of preventive measures. • There are exemptions from the scope of application of the DDA which are not based on proven low risk. This is relevant also to ratings for R.10 to R.12, R.15, R.18, R.19, c.22.1, R.23, c.26.2, R.27, R.28 and R.35. • The responsibility of the investigating officer (internal auditor) does not expressly extend to monitoring compliance with internal controls and supervisory measures.
2. National cooperation and coordination	**C**	
3. Money laundering offences	**LC**	• Definition of property is incomplete - the legislation does not explicitly cover intangible assets.
4. Confiscation and provisional measures	**C**	
5. Terrorist financing offence	**LC**	• The same shortcoming as under R.3 - the legislation does not explicitly cover intangible assets.
6. Targeted financial sanctions related to terrorism & TF	**LC**	• There is no explicit requirement to freeze funds and economic assets without prior notice. • Some deficiencies are also in place with regard to the scope of funds to be frozen, reporting obligation in relation to attempted transaction, as well as the scope of exemptions to be applied. • No guidance is provided to persons subject to the DDA on their obligation to respect the de-listing or unfreezing actions.
7. Targeted financial sanctions related to proliferation	**LC**	• Deficiencies are in place in relation to the scope of funds covered by the freezing obligation, the reporting requirement noting extending to attempted transaction. • There is no clear provisions on permitting additions to accounts. • No guidance is provided to persons subject to the DDA on their obligation to respect the de-listing or unfreezing actions.
8. Non-profit organisations	**LC**	• No risk-based monitoring/supervision, apart from fiscal supervision, is in place in relation to associations.
9. Financial institution secrecy laws	**C**	
10. Customer due diligence	**LC**	• Measures to verify the identity of the BO are risk-based and adequate, rather than "reasonable". • Exemptions available for non-private investment funds, particular types of client accounts operated by lawyers, and persons other than a natural person are not based on proven low risk. • There is no direct requirement to understand the nature of a customer's business and its ownership and control structure. • There is no clear requirement to obtain information on the principal place of business, where different from the registered office. There is no explicit requirement to collect information on all persons holding a senior management position or on powers that regulate and bind the legal entity. • In the case of a member of a board, foundation or trustee, a legal person can be deemed as a BO of the contracting party.

Recommendations	Rating	Factor(s) underlying the rating
		• Banks are required to identify beneficiaries of legal arrangements only when there is a distribution from assets that are entered in their books. • Requirements in respect of beneficiaries of life policies apply only to insurance undertaking. • Not all relevant risk factors must be taken into account when determining whether EDD measures are applicable to the beneficiary of a life insurance policy. • There is no explicit reference to a requirement to manage risk where verification of identity is delayed nor to adopt risk management procedures in all cases where verification is delayed. • For pre-2016 relationships to which enhanced measures did not apply, there were no provisions requiring covered FIs to apply CDD on the basis of materiality and risk, or, when determining appropriate times, to take into account whether and when CDD measures had previously been undertaken and the adequacy of the data obtained. • It does not appear that transitional arrangements apply in respect of some business relationships established prior to 1 January 2001. Nor is termination required in such cases. • It is not specified that selected simplified measures where low risks are identified must be commensurate with risk.
11. Record keeping	**LC**	• There is no explicit requirement to keep the results of any analysis undertaken as part of CDD measures. • There is no explicit requirement to be able to reconstruct individual transactions. • Records must be available within a "reasonable timescale" rather than "swiftly".
12. Politically exposed persons	**LC**	• The definition of PEP excludes a natural person who was entrusted with a prominent public function from the first anniversary of relinquishing that role. • The definition of "associate" does not include a case when a person has joint BO of a legal entity that has been set up for the de facto benefit of a PEP.
13. Correspondent banking	**LC**	• The definition for shell banks requires financial groups to be "regulated" but not explicitly subject to effective consolidated supervision.
14. Money or value transfer services	**C**	
15. New technologies	**PC**	• There is no explicit requirement to assess risk before new products and practices are launched. • The responsibility of the investigating officer (internal auditor) does not expressly extend to monitoring compliance with internal controls and supervisory measures. • There is no general regulation of transfers of VAs nor overriding provision dealing with the provision of financial services related to an issuer's offer and/or sale of a VA. • There is no definition of "qualifying holding" in the TVTG. In the case of a subsequent appointment or acquisition, or subsequent change in the circumstances of a member of a governing body or shareholder/partner, it is not clear that notification must be ex ante notwithstanding that the FMA has no power to remove such a person, other than through withdrawal of the VASP's licence. • The FMA has the power to set aside an offence if it does not believe that a person will re-offend. • The maximum penalty that may be applied by the FMA to first offenders means that the range of sanctions may not be sufficiently proportionate.

Recommendations	Rating	Factor(s) underlying the rating
		• The range of criminal sanctions that may be applied by the Princely Court for failing to report to the FIU under the DDA or violating TFS is not considered to be sufficiently proportionate.
16. Wire transfers	**C**	
17. Reliance on third parties	**LC**	• Reliance may be placed on a delegate domiciled in another EEA member state or third country whose due diligence and record keeping requirements meet Directive (EU) 2015/849 (rather than with R.10 and R.11). • There is no general requirement for the FMA to take account of information on ML/TF risks in the third countries whose requirements for CDD, record keeping, and supervision are considered to meet Directive (EU) 2015/849. • Where there is reliance on group provisions, there is no requirement for higher country risk to be adequately mitigated by the group's AML/CFT policies.
18. Internal controls and foreign branches and subsidiaries	**LC**	• Requirements dealing with host countries with less strict AML/CFT requirements do not apply to EEA member states.
19. Higher-risk countries	**LC**	• The requirement to apply enhanced measures to countries subject to a call from the FATF is not automatic and there is no explicit requirement for the measures selected to be proportionate to the risks.
20. Reporting of suspicious transaction	**LC**	• Shortcomings underlined under the conclusion to R.10 with regard to the scope of application of the DDA are also relevant for this Recommendation.
21. Tipping-off and confidentiality	**LC**	• While it is assumed that directors and officers are covered with executive bodies, the definition of executive bodies is not provided in the legislation.
22. DNFBPs: Customer due diligence	**LC**	• Shortcomings described under R.10, R.11, R.12, c.15.2 are equally applicable to covered DNFBPs. This is the case also for R.17, except that alternative provisions do not apply to DNFBP groups.
23. DNFBPs: Other measures	**LC**	• Shortcomings described under R.19 and R.21, are equally applicable to covered DNFBPs. This is the case also for R.18, except that there is no requirement to establish group strategies and procedures.
24. Transparency and beneficial ownership of legal persons	**LC**	• Except for NPOs, the TF risk assessment does not consider inherent vulnerabilities of different types of legal persons and legal arrangements or their activities. • Group C legal persons and some associations and cooperative societies are not required to be registered. • No explicit requirement is placed on legal persons to maintain documents covering information listed under c.24.3 and ensure that they are available within the country. Similarly, there is no explicit requirement for this information to be held post dissolution. • There are cases where limited liability companies and establishments are not required to maintain a register of shareholders. Cooperative societies, European cooperative societies and trust enterprises are not required to maintain such a register. • Information listed under c.24.3 must be updated "without delay", rather than on a timely basis. Where an obligation to notify a change is not fulfilled, the Commercial Register Division must first request that the required change or deletion be notified within 14 days. • The obligation for partnerships to enter their BO information and extension of the definition of BO of a foundation took effect on 1 October 2021. Auxiliary funds, unregistered partnerships, communities of property, consortia silent partnerships,

Recommendations	Rating	Factor(s) underlying the rating
		homesteads and entailed estates and simple communities of rights are not covered by the register of BO. • There is no specific power available to a legal person that believes that a BO has not provided all necessary information, nor any direct sanction applicable to a BO who does not provide such information. • Insufficient measures are in place to ensure that companies with commercial operations cooperate to the fullest extent possible. • There is no requirement for legal persons to maintain BO information post dissolution. • Restrictions on bearer shares do not apply to certain types of investment funds. Nor do they expressly deal with bearer share warrants. • Mechanisms in place do not sufficiently ensure that nominee shares and nominee directors are not misused (c.24.12). • No penalty is directly applicable for failing to update information. • The average execution time for MLA requests cannot be considered "rapid". • Neither the Office of Justice nor the Court of Justice formally monitor the quality of assistance received in responses to requests for information.
25. Transparency and beneficial ownership of legal arrangements	**LC**	• In the case of a trust, it is not completely clear who has responsibility to report BO information to the Office of Justice. • Communication of BO information for a trust may take up to one year and 30 days. • The average exercise execution time for MLA requests cannot be considered "rapid". • The maximum penalty that may be applied by the FMA to first offenders means that the range of sanctions may not be sufficiently proportionate.
26. Regulation and supervision of financial institutions	**LC**	• There is an insufficient legal basis in the E-Money Act and Payment Services Act for the FMA to prevent management by criminals (or associates of criminals). • For exchange bureaux, it is not clear what statutory provisions are in place to deal with associates of criminals. • It has not been clearly demonstrated that the regulation and supervision of core principles institutions is in line with the core principles which are relevant to AML/CFT. • There is no explicit legislative basis for supervising groups that have a Liechtenstein parent. • The authorities have not clearly explained how the diversity and number of FIs is considered when determining frequency and depth of supervision. The degree of discretion afforded to covered FIs is not specifically considered when assessing risk profile.
27. Powers of supervisors	**LC**	• Apart from a more general power, the FMA does not have an explicit power to conduct inspections to supervise compliance with Regulation (EU) 2015/847. • The term "circumstances exist that appear to endanger the reputation of the financial centre" is not defined. • The maximum penalty that may be applied by the FMA to first offenders means that the range of sanctions may not be sufficiently proportionate.
28. Regulation and supervision of DNFBPs	**PC**	• Statutory provisions are not in place to exclude directors and key function holders of casinos that are associates of criminals. • The exercise of AML/CFT functions by the Chamber of Lawyers (self-regulatory body) is subject only to limited supervision. • It is not clear what statutory provisions are in place to prevent *associates* of criminals holding ownership interests or

Recommendations	Rating	Factor(s) underlying the rating
		management functions in a DNFBP or to prevent the accreditation of lawyers that are *associates* of criminals (c.28.4). • The maximum penalty that may be applied by the FMA to first offenders means that the range of sanctions may not be sufficiently proportionate.
29. Financial intelligence units	**LC**	• For domestic and international cooperation, FIU may conclude agreements only after consulting with competent government member. This, from the technical compliance point, in its turn undermines the overall independence of the FIU.
30. Responsibilities of law enforcement and investigative authorities	**C**	
31. Powers of law enforcement and investigative authorities	**C**	
32. Cash couriers	**LC**	• There is no declaration or disclosure system at the border between Switzerland and Liechtenstein. • The disclosure system entitles the National Police to demand information only if the amount of transferred cash is at least CHF 10 000 or the equivalent in a foreign currency unless there is a suspicion of ML/TF. There is no provision to demand information on cash below CHF 10 000 in case of false disclosure or when information is withheld.
33. Statistics	**LC**	• There is no explicit requirements for keeping statistics on property other than funds which is seized and confiscated.
34. Guidance and feedback	**C**	
35. Sanctions	**PC**	• The range of criminal sanctions that may be applied by the Princely Court for failing to report to the FIU under the DDA or violating TFS is not considered to be sufficiently proportionate. • The maximum penalty that may be applied by the FMA to first offenders means that the range of sanctions may not be sufficiently proportionate.
36. International instruments	**C**	
37. Mutual legal assistance	**LC**	• legislation does provide explicit provisions which require confidentiality of MLA requests and the information contained in them. • For states which are not parties to ECMA, dual criminality is a condition for rendering assistance.
38. Mutual legal assistance: freezing and confiscation	**C**	
39. Extradition	**C**	
40. Other forms of international cooperation	**LC**	• There is no requirement on the FMA to inform a foreign supervisor that it (FMA) is obliged to share information domestically, although the FMA does so as a matter of good practice. • Stricter rules apply on cooperation of the National Police with non-EU members.

GLOSSARY OF ACRONYMS[59]

	DEFINITION
AEOI	Automatic exchange of information in tax matters
AML	Anti-money laundering
Art.	Article
AT	Assessment team
BNI	Bearer negotiable instrument
BO	Beneficial owner
bVOK	Inspection conducted by auditor and commissioned by FMA
CARIN	Camden Asset Recovery Inter-Agency Network
CC	Criminal code of 24 June 1987
CDD	Customer due diligence
CFT	Combating the financing of terrorism
CPC	Code of Criminal Procedure of 18 October 1987
DDA	Law of 11 December 2008 on Professional Due Diligence for the Prevention of Money Laundering, Organised Crime and Financing Terrorism
DDO	Ordinance of 17 February 2009 on Profession Due Diligence for the Prevention of Money Laundering, Organised Crime and Financing Terrorism
DNFBPs	Designated non-financial businesses and professions
DPMS	Dealers in precious metals and stones
DPRK Ordinance	Ordinance on Measures against the Democratic People's Republic of Korea
EDD	Enhanced customer due diligence
EEA	European Economic Area
EOIR	Exchange of information on request for tax purposes
EU	European Union
eVOK	FMA inspection
FATCA	Foreign Account Tax Compliance Act
FATF	Financial Action Task Force
FI	Financial institution
FIU	Liechtenstein Financial Intelligence Unit

59 Acronyms already defined in the FATF 40 Recommendations are not included into this Glossary.

FMA	Financial Market Authority
FMA Act	Financial Market Authority Act
GDPR	General Data Protection Regulation
GRECO	Group of States against Corruption
GVA	Gross valued added
IFC	International financial centre
IO	Immediate outcome
IOSCO	International Organisation of Securities Commissions
Iran Ordinance	Ordinance on Measures against the Islamic Republic of Iran
ISA	International Sanctions Act
ISIL/Al-Qaida Ordinance	Ordinance on Measures against Persons and Organisations associated with ISIL (Da'esh) and Al-Qaida
LEA(s)	Law enforcement agency/authority
MER	Mutual evaluation report
ML	Money laundering
MLA	Mutual legal assistance
MLA Act	Law of 15 September 2000 on International Mutual Legal Assistance in Criminal Matters (Mutual Legal Assistance Act, RHG)
MOU	Memorandum of understanding
MVTS	Money or value transfer services
NPO	Non-profit organisation
NRA	National risk assessment
OECD	Organisation for Economic Co-operation and Development
OFAC	US Office of Foreign Assets Control
OPP	Office of the Public Prosecutor
PEP	Politically exposed person
Person(s) subject to DDA	Entities covered by Art. 3 of the DDA
PF	Proliferation financing
PGR	Persons and Companies Act
PPP	Public-private partnership

PROTEGE WG	The Working Group on the Prevention of Money Laundering, Terrorist Financing and Proliferation
PSP(s)	Payment service providers
R.	Recommendation
RBA	Risk based approach
SARs/STRs	Suspicious activity/ transaction reports
SchlTPGR	Final part to the PGR
SDD	Simplified customer due diligence
SECO	Swiss State Secretariat for Economic Affairs
SEOI	Spontaneous exchange of information in tax matters
SoF	Source of funds
SoW	Source of wealth
STIFA	Foundation Supervisory Authority
Taliban ordinance	Ordinance on Measures against Persons and Organisations associated with the Taliban
TC	Technical compliance
TCSP(s)	Trust and company service provider(s)
Terrorism ordinance	Ordinance of 16 June 2020 on Measures against Certain Persons and Organisations to Fight Terrorism
TF	Terrorism financing
TFS	Targeted financial sanctions
TVTG	Token and TT Service Providers Act
UN	United Nations
United States/US	United States of America
UNSCR(s)	United Nations Security Council Resolutions
VA(s)	Virtual assets
VASP(s)	Virtual asset service provider(s)
VLGST	Association of Liechtenstein Charitable Foundations
VwbPV	Ordinance on the Register of the BO of Legal Entities
WwbPG	Act on the Register of the BO of Legal Entities

www.coe.int/MONEYVAL

May 2022

Anti-money laundering and counter-terrorism financing measures

Liechtenstein

Fifth Round Mutual Evaluation Report

This report provides a summary of AML/CFT measures in place in Liechtenstein as at the date of the on-site visit (6 to 17 September 2021). It analyses the level of compliance with the FATF 40 Recommendations and the level of effectiveness of Liechtenstein AML/CFT system and provides recommendations on how the system could be strengthened.