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(2018)16

Anti-money laundering and counter-terrorist financing measures

Lithuania

Fifth Round Mutual Evaluation Report

December 2018

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 Lithuania was adopted by the MONEYVAL Committee at its 57th Plenary Session (Strasbourg, 3 – 7 December 2018).

TABLE OF CONTENTS

EXECUTIVE SUMMARY

1. This report provides a summary of the anti-money laundering (AML) and countering the financing of terrorism (CFT) measures in place in Lithuania as at the date of the on-site visit (7-18 May 2018). It analyses the level of compliance with the Financial Action Task Force (FATF) 40 Recommendations and the level of effectiveness of Lithuania's AML/CFT system, and provides recommendations on how the system could be strengthened.

Key Findings

- Lithuania's overall understanding of money laundering (ML) and financing of terrorism (FT) risks is limited as it largely depends on a national risk assessment (NRA) completed in 2015, which was found by the assessment team not to be comprehensive enough. Despite the various shortcomings identified in relation to the NRA, the understanding of certain risks at institutional level is more developed, particularly in relation to the use of cash, non-resident business, organised criminality, fictitious companies and FT. Lithuania has taken steps to address some identified threats and vulnerabilities, with concrete results e.g. reduction in tax evasion and the shadow economy. Lithuania has strong national co-ordination mechanisms in place in relation to ML and FT but not proliferation financing (PF).

- In recent years, as a result of greater enforcement of prosecutorial policies, major efforts have been made to target ML as an offence worth pursuing in its own right, in relation to criminal activity posing the highest ML threat. While the number of ML investigations has declined, there has been marked improvement in the ability of law enforcement authorities (LEAs) to investigate complex ML cases. In 2017 and 2018, some major ML convictions were achieved, involving substantial sums and complex laundering schemes. However, most ML convictions are for self-laundering. While a conviction for a predicate offence is not necessary to achieve a ML conviction, there is still some uncertainty as to the level of evidence that would be needed to convince the judiciary that funds derive from criminal activity in the absence of a criminal conviction. It is therefore not surprising that the number of third party/stand-alone ML convictions is limited. Sanctions have the potential to be dissuasive but have not been used effectively. There have only been few ML convictions involving legal persons.

- Depriving criminals of proceeds of crime is a policy objective endorsed at the highest levels. LEAs and prosecutors are aware of and implement the binding recommendations on financial investigations issued by the Prosecutor General (PG). The level of sophistication of financial investigations to trace proceeds of crime has improved and the amount of provisionally seized assets has increased considerably. The volume of confiscated assets remains somewhat modest. The absence of a sound mechanism at the border to identify suspicious transportation of cash at the borders and confiscate such cash raises significant concern, in view of the risks that Lithuania faces.

- The Financial Intelligence Unit (FIU) has a reasonably thorough analysis procedure. LEAs have used the analytical products of the FIU to pursue ML and associated predicate offences to some extent. However, they do not exploit the full potential of the FIU. There are factors which may limit the effectiveness of the FIU's analysis process, particularly the lack of advanced IT analytical tools, limited human resources and absence of a prioritisation mechanism for suspicious transaction reports (STRs). While the number of STRs has increased, the overall quality is still not up to a satisfactory level. It is positive that LEAs have used financial intelligence generated through financial

investigations carried out at the intelligence stage to pursue unlawful enrichment and tax evasion, although to a lesser extent ML.

- Financial institutions (FIs) have a good understanding of ML/FT risks and are aware of their anti-money laundering/countering financing of terrorism (AML/CFT) obligations, although major weaknesses have been observed in some money and value transfer services (MVTS) and currency exchange offices, especially in relation to TFS obligations and FT risks. Understanding of ML/FT risks among designated non-financial businesses and professions (DNFBPs) is insufficient, especially in the real estate sector and traders over EUR 10,000 in cash. The application of CDD measures in the financial sector (especially banks) is good, except for difficulties in verifying BOs of foreign legal persons. CDD by DNFBPs is of a lower quality. Training is deemed insufficient by the private sector, especially non-bank FIs and DNFPBs.

- Licensing controls undertaken by the BoL in relation to FIs are very good. This is less so the case with respect to DNFBP supervisors, also as a result of the absence of registration requirements for company service providers (CSPs), real estate agents and accountants. While the BoL and the FIU have a good understanding of ML risks, DNFBP supervisors have a limited understanding. The BoL has increased the level of supervision significantly during the last two years with some strong elements of risk-based supervision. Risk-based approaches and the levels of supervision undertaken require improvement by most of the DNFBP supervisors. The level of sanctions applied by the BoL has generally been commensurate with its supervisory findings. There are very good elements of effectiveness and dissuasiveness of sanctions although the regime is not yet fully effective and dissuasive. In relation to DNFBPs, the application of the sanctions framework is at a relatively early stage of development.

- ML/FT risks posed by Lithuanian legal entities have not been assessed. However, there is universal agreement among the authorities that fictitious private limited liability companies pose the highest risk. The mechanism which ensures that beneficial ownership (BO) information of legal entities is maintained and made available to competent authorities relies on customer due diligence (CDD) measures applied by the private sector, mainly banks. The mechanism is broadly adequate. Basic information is available on all types of legal persons. Shareholder information is not available on certain types of legal persons. There is no system to ensure that the information kept by the registry is kept accurate and current.

- Authorities have an uneven but broadly adequate understanding of FT risks, consistent with Lithuania's risk profile. There have only been two FT cases in Lithuania. One resulted in a FT conviction. The other is still on-going. While there have been seven terrorism related investigations, no financial investigations were carried out alongside these investigations. There appear to be mechanisms in place for the identification, investigation and prosecution of FT. However, the skills required to deal with such cases need to be developed further. The Customs Service does not have the specific power to stop and restrain currency at the borders in order to ascertain whether evidence of ML/FT may be found. In addition, MVTS providers may not be submitting relevant FT suspicions. Both of these circumstances may result in the non-detection of FT.

- Although no funds have been frozen and the legal framework for targeted financial sanctions (TFS), both for FT and PF, is not fully in line with the Standards (in particular, EU procedures create delays in transposing designations), Lithuania displays elements of an effective TFS system. FIs are aware of UN and EU designations and have customer and transaction screening systems. However, DNFBPs demonstrated limited understanding of TFS obligations. There is no formal procedure to

identify targets for designations and no designation has been made or proposed. The operational framework for the implementation of TFS by the authorities lacks clarity. Although there is no dedicated interagency mechanism, a weekly coordination meeting takes place at the ministerial level on PF-related policy issues. Outreach is provided to the private sector but remains insufficient. Supervisors exhibited limited proactivity in relation to PF-related TFS obligations and evasion challenges.

- Based on a sound legal and procedural framework, Lithuania exchanges information with foreign partners in a comprehensive, proactive and timely manner, both upon request and spontaneously, and in line with its risk profile. The mutual legal assistance (MLA) provided is of good quality as evidenced by the feedback provided by the global network. Lithuania actively seeks international co-operation from other states. This has resulted in convictions and the seizure and confiscation of proceeds of crime, as evidence by various case studies provided to the assessment team. Informal co-operation is conducted effectively.

Risks and General Situation

2. The financial sector in Lithuania is bank-centric (79.2 % of the financial system assets), and is largely concentrated around three foreign-owned banks. The banking services are mainly traditional and include loans and deposits. Banks have been reducing their non-resident customer base for de-risking purposes; and the number of higher risk non-resident customers appears to be very low. In recent years, the Bank of Lithuania has aimed to create an attractive regulatory environment to foreign finance institutions and Fintech start-ups in the country. In 2014, a residence-by-investment programme was also established to attract foreign business.

3. While there is no information on the volume of foreign proceeds invested in or flowing through Lithuania, the NRA notes that the main domestic sources of criminal proceeds are corruption, fraud (including tax fraud), drug trafficking and smuggling of goods. Organised crime (involved in smuggling of goods, drug trafficking and fraud) maintains a strong presence in Lithuania. The significant shadow economy in Lithuania, which is exacerbated by tax offences, and combined with the widespread use of cash, constitutes another important vulnerability. In the financial sector, the NRA cites the increase of technologies in money transfers and the use of cash as the main vulnerabilities. Major vulnerabilities are also found in relation to formal and informal remittances, which play an important role in Lithuania's economy. The DNFBP sector as a whole constitutes a vulnerability due to its poor understanding of ML/FT risks and implementation of AML/CFT requirements.

4. The authorities assess the terrorist threat as low in Lithuania. There has only been one FT conviction. While FT is considered to have a low expectancy level, the NRA notes that (foreign) residents may support known terrorist organisations abroad and lists "lone wolf" terrorism (involving self-financing) as a high-risk priority.

Overall Level of Effectiveness and Technical Compliance

5. Since the last evaluation, Lithuania has taken steps to improve its AML/CFT framework. In 2013, the Criminal Code was amended to explicitly criminalise the financing and support of terrorism and extend the list of activities which are punishable as ML. Amendments to the AML/CFT Law were adopted in 2014 to reorganise the STR regime and address deficiencies concerning CDD and record

keeping obligations. Further amendments to the AML/CFT Law were adopted on 13 July 2017 to transpose the Directive of the European Parliament and Council (EU) 2015/849. The amendments extended the scope of obliged entities and reinforced sanctions for breaches of AML/CFT preventive measures. However, some deficiencies remain in Lithuania's technical compliance framework, in particular in relation to risk assessment, national cooperation and coordination and targeted financial sanctions.

6. Lithuania has demonstrated a substantial level of effectiveness in engaging in international cooperation. A moderate level of effectiveness has been achieved in all the other areas covered by the FATF Standards.

Assessment of Risks, coordination and policy setting (Chapter 2 - IO.1; R.1, R.2, R.33)

7. Lithuania's understanding of ML/FT risks is limited and high-level in nature. The understanding of risks is largely based on the 2015 NRA, which presents a number of weaknesses. The document is informed by an insufficient range of information sources and the analysis remains high-level in nature. The NRA focuses mainly on threats and vulnerabilities, leaving aside the resulting risks. It does not describe the main ML methods, trends and typologies or give adequate consideration to cross-border threats and the Fintech sector. The understanding of risks at the institutional level is more developed concerning issues such as the use of fictitious companies and the use of cash.

8. Based on an action plan which was completed in 2017, Lithuania has taken steps to address a number of threats and vulnerabilities, with concrete results, in particular, in reducing tax evasion and the shadow economy. However, further efforts are needed to mitigate other significant vulnerabilities, in particular in relation to investigation and prosecution of ML and AML/CFT supervision.

9. Lithuania has strong co-ordination mechanisms in place, including the AML/CFT Coordination Group and many agreements on exchange of information between authorities at the operational level. However, there are no co-ordination mechanisms with respect to PF.

Financial Intelligence, Money Laundering and Confiscation (Chapter 3 - IOs 6-8; R.3, R.4, R.29-32)

10. The FIU has a reasonably sound analysis procedure and the products disseminated by the FIU were effectively used by LEAs to some extent to initiate pre-trial investigations. The FIU has broad and unhindered access to information sources. The FIU regularly makes use of these sources in the course of its analysis. Analysts appear knowledgeable and have produced complex analysis. There are some factors which have a negative impact on the effectiveness of analysis: insufficient human resources and the lack of advanced IT tools and prioritisation mechanisms for STRs.

11. The number of STRs has increased considerably in the period under review, but their overall quality remains unsatisfactory. MVTS, real estate agents, notaries and CSPs have filed few or no STRs, which is a concern in light of the ML/FT risks they face. No analysis has been initiated on the basis of customs declarations.

12. It is positive that LEAs have used financial intelligence generated through financial investigations carried out at the intelligence stage to pursue unlawful enrichment and tax evasion, although to a lesser extent ML.

13. At the beginning of the period under review, opportunities to identify ML in the course of predicate offence investigations were not explored to the greatest extent possible, the degree to which ML was targeted by each LEA varied and the approach to proactively pursue ML cases was fragmented. Latterly, concrete efforts have been made to target ML as an offence worth pursuing in its own right, separately from the prevention and repression of predicate criminality, as a result of greater enforcement of prosecutorial policies, which classify ML as a high priority offence. This is supported by a number of on-going investigations presented to the assessment team, some of which have already resulted in ML convictions. However, a national ML-specific operational policy is needed to ensure a more uniform and effective approach across all LEAs involved.

14. In 2017 and 2018, some major ML convictions were achieved, involving substantial sums and complex laundering schemes. However, most ML convictions are for self-laundering. While a conviction for a predicate offence is not necessary to achieve a ML conviction, there is some uncertainty as to the level of evidence that would be needed to convince the judiciary that funds derive from criminal activity. The use of circumstantial evidence to prove that the launderer knew that the property derived from criminal activity is not always accepted by the courts, although there are clear precedents. It is therefore not surprising that the number of third party and stand-alone ML convictions is limited.

15. The sanctions under Article 216 have the potential to be dissuasive. However, sanctions have not been used effectively and dissuasively. Many of the sentences involved a fine, often lower than the laundered proceeds. Most imprisonment sentences were suspended. There have not been many ML convictions for legal persons, despite the fact that legal persons feature recurrently in cases presented by the authorities.

16. Depriving criminals of proceeds of crime is a policy issue endorsed at the highest levels within the prosecutorial and law enforcement structures in Lithuania. The complexity and sophistication of financial investigations appears to have improved in the last couple of years. It has now become increasingly common, when investigating complex proceeds-generating crimes, to set up joint investigation teams, involving case investigators, intelligence officers and financial specialists. However, further progress is needed to continue enhancing the quality of financial investigations, especially within the State Investigation Service.

17. Data on the volume of assets seized and confiscated in relation to ML and other predicate offences and on restitution to victims demonstrates a visible improvement in the implementation of seizure and confiscation requirements, especially when compared to the situation at the time of the 4th Round MER adopted in 2012. While the volume of seized assets has increased significantly, the volume of confiscated assets remains somewhat modest.

18. The absence of a sound mechanism at the border to identify suspicious transportation of cash at the borders and confiscate such cash raises significant concern.

Terrorist Financing and Financing Proliferation (Chapter 4 - IOs 9-11; R.5-8)

19. The authorities involved in the prevention and investigation of FT and terrorist-related crimes have a broad understanding of FT risks and threats, which is consistent with the level of risk present in the country. The SSD has the most advanced understanding of FT risks.

20. There have only been two FT cases in Lithuania. One resulted in a FT conviction. The other is still on-going. There have been seven terrorism related investigations. No financial investigations were carried out alongside these investigations. While there appear to be mechanisms in place for the identification, investigation and prosecution of FT, the skills required to deal with such cases need to be developed further.

21. The Customs Service does not have the specific power to stop and restrain currency at the borders in order to ascertain whether evidence of ML/FT may be found. In addition, MVTS providers may not be submitting relevant FT suspicions. Both of these circumstances may result in the non-detection of FT.

22. While the Public Security Programme (2015-2025) contains a specific goal relating to terrorism and FT, it does not appear that an action plan has been developed to implement this goal in practice. Therefore, the assessment team could not determine that the investigation of FT would be integrated, and used to support, national counter-terrorism strategies and investigations.

23. The sanctions provided in the CC for FT offences appear to be proportionate and dissuasive. In the one court decision related to FT the most severe punishment was applied. The instrument of the crime was confiscated.

24. Lithuania has identified potential vulnerabilities within the NPO sector. Although NPOs are only supervised for tax-related issues, the SSD closely monitors those NPOs that could be misused for FT purposes. Outreach to NPOs is insufficient.

25. The legal framework for FT- and PF-related TFS is not fully in line with the Standards. In particular, EU procedures impose delays in transposing designations (except for Iran). Although no funds have been frozen, Lithuania displays elements of an effective system to implement TFS pursuant to UNSCRs 1267 and 1373. FIs, including Fintech operators, are aware of UN and EU designations and have systems in place to monitor customers and transactions against the relevant lists. DNFBPs demonstrated limited understanding of these obligations. Lithuania does not have formal procedures to identify targets for designations and has not proposed or made any designations. The operational framework governing the implementation of TFS by the authorities lacks clarity.

26. While no PF-related funds have been frozen, awareness of PF-related TFS is widespread in the financial sector, in particular among banks. In many cases banks demonstrated a strict compliance approach that has resulted in refusing payments not subject to TFS (e.g. any transaction linked to Iran). As with FT, DNFBPs show a limited awareness of PF lists and follow a seemingly sporadic screening approach. The Ministry of Foreign Affairs is the lead agency for countering PF. Although there is no dedicated interagency mechanism, a weekly coordination meeting on takes place at the ministerial level on PF-related policy issues. The Ministry of Economy, as the licensing authority for dual-use goods, regularly holds workshops for industry associations, in which updates on TFS lists are provided. Both the FIU and the MFA have adopted a more targeted approach in assisting banks to comply with their PF-related TFS obligations, including to prevent sanctions evasion. Additional outreach and typologies would be beneficial. Supervisors exhibited limited proactivity in relation to PF-related TFS obligations and evasion challenges.

Preventive Measures (Chapter 5 - IO4; R.9-23)

27. Banks have a high-level of understanding of ML/TF risks and are aware of their AML/CFT obligations. This is broadly the case for other financial institutions, but major weaknesses have been observed in some MVTS and currency exchange offices, especially in relation to TFS obligations and FT risks. Understanding of ML/FT risks among the DNFBPs sector is not sufficient, especially in the real estate sector and traders over EUR 10,000 in cash. The application of CDD measures in the financial sector (especially banks) is good, except for difficulties in verifying BOs. CDD by DNFBPs is of a lower quality, with very limited understanding of the minimum requirements set by the law in some cases. Overall, REs understand the STR procedure, but reports from MVTS, currency exchange offices, real estate agents, notaries and lawyers are limited in light of their risk profile. Training is deemed insufficient by the private sector, especially non-bank FIs and DNFPBs.

Supervision (Chapter 6 - IO3; R.26-28, R. 34-35)

28. The BoL applies very good controls in relation to the licensing of FIs to prevent criminals from holding, or being the BO of, a significant or controlling interest or holding a management function in FIs. The BoL has a good understanding of ML risk within banks, and the products and services offered by FIs and a general understanding of ML risks in the sectors it supervises. It broadly understands FT risk. The BoL is a proactive supervisor and has increased the level of supervision significantly during the last two years. It has some strong elements of risk-based supervision and it is moving towards both a comprehensive risk-based approach and a level of supervision in line with risks. The level of sanctions applied by the BoL has generally been commensurate with its supervisory findings. There are very good elements of effectiveness and dissuasiveness of the sanctions regime although it is not yet fully effective and dissuasive.

29. Licensing controls in relation to DNFBPs vary, including an absence of registration requirements for CSPs, real estate agents and accountants. In general, DNFBP supervisory authorities except the FIU (which has a generally good understanding of the ML/FT risks of real estate agents and accountants) have a developing understanding of risk. The extent of AML/CFT supervision and the degree this is risk-based varies, with the GCA, the FIU and the LAO being most proactive authorities; overall, risk-based approaches and the levels of supervision undertaken require improvement. Some sanctions have been applied by DNFBP supervisory authorities and the courts in relation to DNFBPs. Overall, the application of the frameworks and their effectiveness is at a relatively early stage of development.

Transparency of Legal Persons and Arrangements (Chapter 7 - IO5; R. 24-25)

30. While Lithuania has not conducted a formal assessment of risks posed by legal persons, it is universally understood by competent authorities that the use of fictitious private limited companies in criminal schemes constitutes a significant ML/FT risk.

31. The Register of Legal Entities (RLE) maintains basic information on all types of legal persons, which is publicly-available. This ensures that access to competent authorities is timely. However, there is no system to ensure that the information is kept accurate and current. Shareholder information on the vast majority of legal persons is available either from the RLE or at the Information System of Members of legal Entities ("JADIS"), which jointly hold information on 83.8% of legal persons registered in Lithuania. Shareholder information in JADIS is available to competent

authorities (free of charge) and to reporting entities (against a fee), though this information is not verified to ensure that it is accurate and current.

32. The mechanism to ensure availability of BO information relies on CDD performed by private sector entities, mainly banks, which verify information on the basis of information maintained at the RLE and JADIS. Given that most legal persons registered in Lithuania are owned and controlled by Lithuanian natural (81.1%) and legal persons (6.6%), this mechanism is broadly adequate with respect to legal persons whose information is contained in JADIS. In fact, competent authorities have not encountered any difficulties in obtaining BO information in this manner. However, there remains a small gap with respect to some legal persons in relation to which information is not available at the RLE or JADIS (16.2% of all legal persons). Additionally, there is no system of verification of information entered into JADIS. Furthermore, there is no complete information on the number of Lithuanian corporate shareholders whose shareholders are legal persons registered outside of Lithuania.

33. Lithuania has implemented effective mitigating measures against the use of fictitious private limited liability companies for criminal purposes, which are considered to pose highest risk, compared to other legal persons. The STI actively monitors information on VAT payers to identify fictitious companies. Many cases involving the use of fictitious companies have been prosecuted. The FIU conducts typology exercised to assist in determining the scale of the problem and forward cases to LEAs.

International Cooperation (Chapter 8 - IO2; R. 36-40)

34. Lithuania has a sound legal and procedural framework to exchange information and cooperate with its foreign counterparts in relation to ML, associated predicate offences and FT. Information is exchanged comprehensively, proactively and in a timely manner, both upon request and spontaneously. The evaluation team received positive feedback from the AML/CFT global network in relation to the quality and timeliness of assistance provided by Lithuania.

35. Lithuania actively seeks international co-operation from other states. This has resulted in convictions and the seizure and confiscation of proceeds of crime, as evidence by various case studies provided to the assessment team.

36. Effective cooperation between Lithuania and other EU Member States is well-developed, especially with the other Baltic States. Regular cooperation based on UN instruments and bilateral agreements also takes place outside of the EU, especially with neighbouring countries.

37. On average, requests for MLA are processed within 1 to 4 months, depending on the nature of the request, the type of assistance requested and the complexity of the request. Urgent requests are executed within shorter time-frames.

38. The authorities advised that not a single MLA request related to ML/FT was refused in the period under review. This was also confirmed by the AML/CFT global network. In the few instances where MLA was not provided in relation to predicate offences, the authorities explained that this was due to deficiencies in the form and content of a request as laid down in international treaties, statute of limitations and/or requests relating to acts which did not involve criminal liability.

39. While extradition figures show that only a portion of extradition requests is actually executed, the authorities explained that a significant part of these requests involved persons who did not reside

in Lithuania. The others were refused on the grounds that Lithuania cannot extradite its own nationals.

40. In terms of informal co-operation, the FIU has a broad legal basis for the exchange of information with its foreign counterparts. Spontaneous information is regularly exchanged. The assistance provided is considered effective in terms of timeliness and quality. LEAs are also active in the sphere of informal cooperation through direct communication via Europol, Interpol, SIENA and CARIN. The creation of joint investigative teams between Lithuanian LEAs and their foreign counterparts on large scale cases has become increasingly common. The BoL makes full use of a large number of bilateral and multilateral agreements to exchange information with its counterparts, especially in relation to AML/CFT on-site inspections.

Priority Actions

1. Lithuania should, as a matter of priority, conduct the next iteration of the NRA, which should:

a) involve supervisory authorities, especially the BoL, more directly – for instance all supervisory authorities should be involved in the discussions of working groups set up to discuss threats and vulnerabilities and not just be required to complete questionnaires;

b) be based on a more comprehensive set of qualitative and quantitative information sources – for instance, information from the SSD on FT risks, information from the BoL on the risks posed by cash and non-resident customers, information from the FIU on typologies and more detailed statistics;

c) consider to a larger degree the cross-border ML threat (at least include an assessment of: financial flows to and from high risk countries, MLA requests received and sent, international informal requests from and to FIU and LEA, STRs and cash declarations), the use of fictitious companies (by analysing information from LEAs), the use of cash (by analysing information from the FIU, the BoL, the Customs Department and the STI);

d) assess the vulnerabilities of the Fintech sector;

e) for the purpose of the assessment of FT risks, separately consider the risks of movement, collection, provision and use of funds and include an assessment of the vulnerabilities of financial instruments and risks related to flows to high-risk jurisdictions.

2. Establish mechanisms for the co-ordination of PF actions. The authorities may wish to extend the mandate of the AML/CFT Coordination Group to cover PF issues and the membership of the Group to include other relevant stakeholders, such as the MoE.

3. The use of financial intelligence developed through financial investigations at the intelligence stage should be widened to, inter alia, target ML and FT elements (in addition to unlawful enrichment and tax-related offences[1]), follow the trail of potential proceeds of crime and identify other involved parties, such as beneficiaries of transactions, to establish new or additional links and leads for investigations.

4. The authorities should take measures to improve the quality of STRs, including by: 1) determining whether the suspicious indicators need to be further enhanced; 2) holding discussions with banks to ensure that reporting is further aligned with the risks facing Lithuania; 3) assess

[1] The authorities indicated that following the on-site visit measures were taken to update the PG's Recommendations accordingly.

whether the quality and reporting level by each bank are adequate; 4) hold awareness-raising activities with reporting entities facing a higher risk of ML/FT on reporting; 5) provide more systematic feedback to reporting entities on reporting; 6) consider why other reporting entities have not submitted any STRs (other than banks and MVTs); 7) consider whether the limited number of FT STRs is entirely in line with the risks that Lithuania faces.

5. The Customs Department should develop sound mechanisms to be able to detect false or non-declarations and suspicions of either ML or FT (which could arise even where declarations are submitted).

6. The FIU should re-calibrate its analysis and dissemination priorities to focus on the highest ML risks and make more effective use of its limited resources.

7. Enhance the technical capacities (IT tools) of the analysis function of the FIU and ensure that it is adequately resourced in terms of staff. Compliance responsibility should not deprive resources from the analysis section. Compliance matters should be dealt completely separately from the analysis section.

8. Lithuania should strengthen existing law enforcement strategies by developing a ML-specific operational policy which should:

a) clearly set out how each LEA is to identify and initiate ML cases, including through parallel financial investigations both at criminal intelligence and pre-trial stage, on the basis of FIU disseminations, in the course of the investigation of a predicate offence; and through the sharing of information between LEAs; and

b) include measures to (1) pro-actively identify ML elements at the earliest stages of suspicion and consequently initiate ML investigation rather than focussing only on unlawful enrichment; and (2) trace the sources and destination of proceeds of crime.

9. Law enforcement efforts should be in line with the ML risks. In particular, LEAs should continue targeting more complex and sophisticated types of ML with special attention to cases which involve the misuse of fictitious companies, trade-based ML, fraud, organised crime, corruption and ML related to foreign predicate offences). In complex criminal schemes, LEAs should extend their investigation with the aim of identifying the person(s) who ultimately controls and benefits from the scheme.

10. The PG Recommendations should be updated to improve the ability of LEAs and the Prosecution Service developing 'objective circumstantial and indirect evidence' when proving: (1) that the property is the proceeds of crime, in the absence of a conviction for the underlying crime; and (2) intent and knowledge of the launderer.

11. LEAs and the PGO should continue challenging the judiciary with stand-alone ML cases where it is not possible to establish precisely the underlying offence(s) but where the courts could infer the existence of predicate criminality from adduced facts and circumstances. More cases related to professional third-party ML should also be brought forward.

12. Revise the PG's Recommendations on financial investigations to extend their scope beyond the financial profile of the suspect and include reference to the identification and tracing of movements of the proceeds of crime and identifying the extent of criminal networks and/or the scale of criminality.

13. Strengthen the enforcement of the PG's Recommendations to ensure that all types of property (laundered property, co-mingled, property of equivalent value and instrumentalities) are provisionally restrained and confiscated upon conviction

14. Lithuania should enable targeted financial sanctions relating to FT and PF to be implemented without delay, in line with the FATF Recommendations and introduce a mechanism(s) for the identification of targets for designations in relation to FT UNSCRs.

15. As planned, registration of TCSPs should be introduced and registration and standard setting frameworks should be put in place for real estate agents and accountants. The GCA should develop its existing approach, while other DNFBP supervisors should take additional steps to prevent criminals from holding, or being the beneficial owner of, a significant or controlling interest or holding a management function in DNFBPs.

16. A mechanism should be introduced so that approaches by the supervisory authorities to addressing risk and the development of comprehensive risk-based supervision are coordinated.

17. The BoL and the FIU should use onsite and offsite tools, and the next iteration of the NRA, to enhance their understanding of ML and FT risks relevant to their sectors. Other supervisory authorities should use these tools and the NRA to develop comprehensive understanding.

18. The BoL should enhance its existing risk-based approach and further develop its ML/FT risk assessment in order to ensure that risk-based supervision is comprehensive. DNFBP supervisors should take the significant steps required to achieve comprehensive risk-based approaches to supervision. Systematic AML/CFT training programmes should be developed by the supervisory authorities.

Effectiveness & Technical Compliance Ratings

Effectiveness Ratings (High, Substantial, Moderate, Low)

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

Technical Compliance Ratings (C, LC, PC, NC)

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
PC	PC	LC	LC	LC	PC
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
PC	LC	C	LC	C	C
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	LC	C	LC	C	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	C	LC	LC	PC
R.25 - Transparency & BO of legal arrangements	R.26 – Regulation and supervision of financial institutions	R.27 – Powers of supervision	R.28 – Regulation and supervision of DNFBPs	R.29 – Financial intelligence units	R.30 – Responsibilities of law enforcement and investigative authorities
LC	PC	C	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
LC	PC	LC	LC	LC	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	LC	LC	LC		

MUTUAL EVALUATION REPORT

Preface

1. 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.

2. 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 7 to 19 May 2018.

3. The evaluation was conducted by an assessment team consisting of: Mr Ladislav Majernik, Senior Prosecutor, Acting Head, International Public Law and European Matters, General Prosecutor's Office, Slovak Republic (legal expert), Mr. Vitaly Berehivskyi, Head of Division for Cooperation with Foreign FIUs, Department for Financial Investigations, the State Financial Monitoring Service, Ukraine (law enforcement expert), Ms Anna Pajewska, Chief Specialist, Department of Financial Information, Ministry of Finance, Poland (financial sanctions expert), Mr Richard Walker, Director of Financial Crime Policy and International regulatory Advisor, Policy Council of the States of Guernsey, Guernsey (financial expert), Ms Sona Suvaryan, Analyst, Analysis Division, Financial Monitoring Centre, Central Bank, Armenia (financial expert) with the support from the MONEYVAL Secretariat of Mr Michael Stellini, Mr Panagiotis Psyllos and Mr Jérémie Ogé. The report was reviewed by Mr Giuseppe Lombardo (International Strategic Advisor – Financial Integrity), Ms Tanjit Sandhu (Financial Market Integrity, World Bank) and the FATF Secretariat.

4. Lithuania previously underwent a FATF Mutual Evaluation in 2012, conducted according to the 2004 FATF Methodology. The 2012 evaluation and follow-up reports have been published and are available at https://www.coe.int/en/web/moneyval/jurisdictions/lithuania. That Mutual Evaluation concluded that the country was compliant with 10 Recommendations; largely compliant with 21; and partially compliant with 17. One Recommendation (R.34) was considered to be not applicable. Lithuania was rated compliant or largely compliant with 7 of the 16 Core and Key Recommendations. Lithuania was placed under the expedited follow-up process immediately after the adoption of its 4th Round Mutual Evaluation Report and was removed from the follow-up process in September 2017.

CHAPTER 1. ML/TF RISKS AND CONTEXT

5. Located in the Baltic region of northern-eastern Europe, Lithuania is one of the smallest countries in the continent, covering 65,300 square kilometres. Lithuania shares borders with Latvia in the north, Belarus in the east and south, Poland in the south and the Russian region of Kaliningrad in the southwest. Vilnius is the capital of the country. Lithuania is the most populous of the Baltic countries and its population is 2.87 million (United Nations estimates as of June 01, 2018). Lithuania's GDP is about EUR 41.9 billion (2017 current prices, Eurostat[2]) and its official currency is the Euro.

6. Lithuania is a parliamentary republic with semi-presidential form of government elements. The president of Lithuania is the Head of the State and is elected for a five-year term. The constitution

[2] http://appsso.eurostat.ec.europa.eu/nui/show.do?dataset=nama_10_gdp&lang=en

provides the President with the power to appoint the Prime Minister upon confirmation of the Parliament and, upon Prime Minister's recommendation, of the Council of Ministers, composed by 13 ministries. The president also serves as commander-in chief. The day-to-day administration of the government rests in the hands of the Prime Minister, who heads the Cabinet of Ministers (CoM). Legislative power is vested in the Parliament. A unicameral parliament (Seimas) consists of 141 deputies. The members of the Parliament are elected for a four-year term in free, multi-candidate elections. Lithuania's legal system is based on civil law principles.

7. Lithuania is a member of the European Union, the United Nations, the Council of Europe, the Organisation for Economic Co-operation and Development (OECD), the Organisation for Security and Cooperation in Europe, the World Trade Organisation, the European Bank for Reconstruction and Development, the World Bank, the International Monetary Fund and other international organisations.

ML/TF Risks and Scoping of Higher-Risk Issues

Overview of ML/TF Risks

8. The main sources of criminal proceeds generated domestically are tax fraud, corruption[3], fraud, drug trafficking, smuggling of excise goods and large-scale theft[4]. Domestic proceeds average EUR 60 million per year[5] which represent 0.17% of GDP. Organised crime groups (OCGs) maintain a strong presence in Lithuania and are particularly active in the domain of smuggling of goods, drug trafficking and fraud (e.g. cyber, social engineering)[6]. While the number of recorded predicate offences has been decreasing in recent years, the volume of proceeds has been on the rise, particularly in the last two years. There is no information on the volume of foreign proceeds invested in or flowing through Lithuania[7].

9. The national risk assessment (NRA) identifies two overarching vulnerabilities within the national system; the ineffective identification, investigation and prosecution of money laundering (ML) and shortcomings in the supervision of both the financial and non-financial sectors. Concerning the financial sector, the NRA cites the increase of technologies in money transfers and the use of cash as the main vulnerabilities. With respect to the use of formal and informal remittances, the major vulnerabilities include limited regulation of foreign money value transfer services (MVTS) operating in Lithuania, limited transparency of MVTS operations and weak cash-courier controls at the borders.

---

[3] For instance, two Lithuanian political parties have been officially accused of participating in a large-scale corruption plot, orchestrated by one of the most influential business groups in the country. See, for example, www.occrp.org/en/daily/7043-lithuania-two-political-parties-charged-in-major-corruption-case.

[4] NRA, P. 20.

[5] Figures from the last five years provided by Lithuania in the Effectiveness submission

[6] https://www.mruni.eu/upload/iblock/2ca/17%20Gutauskas.pdf; http://www.thejakartapost.com/news/2014/12/16/lithuanian-arrested-smuggling-crystal-meth.html; http://www.transcrime.it/wp-content/uploads/2016/06/The-Belarusian-Hub-for-Illicit-Tobacco.pdf

[7] There is information which indicates that this might not be uncommon: https://www.reuters.com/article/us-danske-bank-moneylaundering/danske-bank-fined-over-money-laundering-says-expands-internal-probe-idUSKBN1EF18P http://www.independent.co.uk/news/world/europe/lithuanian-prosecutors-open-investigation-into-multi-million-dollar-tax-fraud-by-russian-organised-8460569.html http://www.fntt.lt/data/public/uploads/2017/09/ml_tfp_activities_financial_crime_investigation_service_2016.pdf

The Designated Non-Financial Businesses and Professions (DNFBP) sector as a whole is considered to be vulnerable to abuse due to the sector's lack of awareness of ML/FT risks and poor implementation of (risk-based) anti-money laundering/counter-terrorist financing (AML/CFT) requirements, including the identification/verification of beneficial ownership.

10. According to the financial intelligence Unit (FIU), prevailing trends and patterns of ML involve the use of fictitious companies, money mules, wire transfers, cash deposits and withdrawals, monetary operations through accounts of offshore companies and physical cross-border cash flows[8]. Proceeds of crime are said to be invested in legal businesses such as real estate, construction, transportation and agriculture[9].

11. The terrorism/FT threat in Lithuania is assessed by the authorities to be low. There has only been one terrorism financing (FT) conviction[10]. While FT is considered to have a low expectancy level, the NRA acknowledges that (foreign) persons residing in Lithuania may support known terrorist organisations in other countries and lists "lone wolf" terrorism (involving self-financing) as a high-risk priority. These conclusions appear to be based on hypothetical considerations but also take into account risks arising in neighbouring areas, the evolution of FT risks globally and Lithuania's geographical position. Otherwise, the assessment team did not come across any publicly-available information suggesting that Lithuania faces an elevated risk of FT. Weak cash controls at the border and inadequate application of preventive measures by certain MVTS providers constitute a vulnerability.

Country's risk assessment & Scoping of Higher Risk Issues

12. Lithuania published its first NRA in 2015. The NRA report considers both ML and FT. A high-level AML/CFT Coordination Group created by the order of Prime Minister No 42 of March 2015 co-ordinated the development of the NRA with the assistance of "Deloitte Lietuva". Representatives of most of the participants of the national financial monitoring system participated in the analysis and other work leading up to the final report. Threats, vulnerabilities and institutional gaps were identified and an action plan was drawn up by the authorities and approved in June 2016.

13. Sources of information for the NRA include legislative instruments in Lithuania and international conventions, MONEYVAL reports and recommendations, reports of the Lithuanian FIU, regulatory and supervisory bodies, professional associations responsible for the implementation of AML/CFT legislation, responses to questionnaires and surveys, interviews with stakeholders, statistics on the number of suspicious transaction reports (STRs), sanctions, ML/FT investigations etc., and national and international mass media.

14. The NRA methodology is based on five stages in managing AML/CFT risks: 1) data collection; 2) risk identification; 3) risk assessment; 4) risk response measures; 5) risk management plan. The authorities pointed out that the phase of identification of the risks should be considered in a "dynamic" way as risks are identified through all the stages. The threats and vulnerabilities that have been detected have been analysed in order to establish their characteristics and subsequently

[8]Annual Reports of the Lithuanian FIU (Financial Crimes Investigation Service) available at http://www.fntt.lt/en/money-laundering-prevention/activities/annual-reports/230.

[9] See NRA.

[10] The case related to the support of the terrorist group "The Real Irish Republican Army" operating in Ireland and the UK. The case was referred to the court in 2009 and a final (court of cassation) judgement was rendered in 2017.

categorised in order to establish their nature. Registers were created by the assessors in order to keep track of the data and records regarding the identified threats and vulnerabilities. Each of these were assigned to stakeholders as "risk owners" on the basis of their attributions and responsibilities in order to be managed in an appropriate way.

15. Each threat and vulnerability was assigned a net risk level, which represents the NRA's conclusion for that risk. The 81 risks that affect or may affect Lithuania in matter of ML/FT identified in the NRA received scores from 3 to 13. Those that received a scoring of 10 to 15 were considered high-priority risks, based on the risk-scoring matrix. Based on the risk assessment results, response strategies have been elaborated: 1) mitigation (response for 39 risks); 2) avoidance (response for 13 risks); 3) sharing (response for 8 risks); 4) acceptance (response for 21 risks). Moreover, the identified risks were divided into four AML/CFT sectors, taking into account the Lithuanian AML/CFT system: Law Enforcement Authorities (LEAs), Supervision and Regulatory Sector, Financial Sector and Non-financial sector.

Scoping of Higher Risk Issues

16. The assessment team identified those areas which required an increased focus through an analysis of information provided by the Lithuanian authorities, including the NRA and by consulting various open sources.

17. **The use of cash**: the use of cash in Lithuania is widespread and facilitates tax evasion and exacerbates the shadow economy. The withdrawal, deposit and remittance of cash (either through MVTS or physical transportation) are commonly used in ML schemes. The assessors have focused on (1) the success of the measures taken so far to reduce the shadow economy, tax evasion and related ML; (2) whether the FIU is making effective use of cash transaction reports to identify ML and associated predicate offences; (3) the effectiveness of controls at the borders to detect false/non-declarations and identify ML/FT suspicions; (4) whether the regulation and supervision of MVTS has improved since the completion of the NRA; (5) measures implemented by the financial sector, particularly banks and MVTS, to identify the source of funds in relation to cash transactions.

18. **Non-resident business**: Following the Panama Papers leaks, the Bank of Lithuania conducted a study in 2016 to gauge the extent to which the banking sector (and the largest e-money institution) services customers from international financial centres (IFCs). It was concluded that the exposure was limited and, as a result, the risk arising from non-resident business was assessed to be low. However, the process appears to have focussed exclusively on whether the banking sector had direct business relationships with customers (mainly legal persons) registered in IFCs. The assessment team sought to determine whether Lithuania considered the extent to which legal persons registered in Lithuania form part of complex corporate structures involving legal entities or arrangements registered in IFCs or to identify the number of customers that are legal persons registered in Lithuania which are beneficially owned by non-residents. The assessors have also requested the authorities to provide information on the volume, origin and destination of wire transfers. There are indications that fictitious companies registered in Lithuania, which are beneficially owned by non-residents, have been involved in significant ML schemes[11]. The evaluation team have also explored in detail banks' understanding of these risks and their implementation of beneficial ownership requirements. In addition, given that at the time of the on-site visit Lithuania does not regulate trust

[11] See for instance 2016 Annual Report of the FIU.

and company service providers (TCSPs), the assessors have to determine how fictitious shell companies are incorporated.

19. **Organised crime**: in the NRA it has been noted that LEAs do not have sufficient resources to aggressively pursue the activities of OGCs, despite the considerable threat that they pose. The action plan to address the risks identified in the NRA sets out measures intended to improve law enforcement capabilities in this area, including measures related to seizure and confiscation. The assessors have focussed on whether these measures have already borne concrete results. Statistics provided by the authorities indicate that third party and stand-alone ML convictions are still few and far in between. There are, however, some encouraging signs in terms of confiscation.

20. **Corruption:** The assessment team sought to determine the extent to which corruption has a negative impact on the governance of the supervisory framework and the criminal justice system. In terms of the threat, the assessors have focused particularly on the level of effectiveness of relevant AML/CFT preventive measures (particularly those related to politically-exposed persons (PEPs)) and law enforcement efforts to repress corruption and related ML.

21. **Understanding of FT risks:** the assessors have examined in detail whether the authorities' understanding of FT risk has evolved since the completion of the NRA, in view of new and emerging risks, and determine whether any actions have been taken to address these risks. The assessors have also considered whether there are aspects of the sector which could be abused for FT purposes.

22. **Financial technology (Fintech) and the use of technology:** very little information has been made available on the development of Fintech and the regulatory framework that is now in place in Lithuania. At the time of the on-site visit, the Fintech sector in Lithuania comprised crowd-funding and peer-to-peer lending platforms, which offer access to cheap financing of projects and start-up enterprises, licensed Electronic Money Institutions issuing Electronic Money on Blockchain technology[12], crypto-currency exchanges allowing customers to trade crypto-currencies or digital currencies for other assets, such as conventional fiat money, or different digital currencies, and Initial Coin Offerings (ICO) and Token offerings allowing funding for start-ups in which new digital tokens or coins are issued. Although licences have already been granted to entities (e.g. crowd-funding or peer-to-peer lending platforms), it is not clear whether the authorities have assessed ML/FT-related risks. As mentioned in the section on risk, the NRA identifies the use of technology in money transfers as a high-risk priority area within the financial sector, without specifying either which technologies are particularly risky or the scale of the problem. Clarifications were requested by the assessors. The assessment team also scrutinised the mitigating measures implemented by the financial sector to manage this risk.

23. **Proliferation financing (PF):** One source[13] indicate that a total of 14 incidents involving theft and smuggling of nuclear material have been recorded in Lithuania, all recorded in the years prior to the review period. In half of these cases, Lithuanian citizens were involved in nuclear smuggling, while the rest involved radioactive materials or contaminated metals being transported through Lithuanian territory. Overall, Lithuania was mainly involved in cases of enriched uranium smuggling. No funds or other assets have been frozen under the relevant targeted financial sanctions regimes. The assessors have explored the ability of the private sector to identify funds or other assets of

[12] Blockchain is a large distributed database, a ledger, protected by cryptography (i.e. algorithms which encrypt and de-crypt information) used for the management and record of financial transactions and everything of value between several users (nodes) of a network.
[13] https://www.degruyter.com/downloadpdf/j/lasr.2016.14.issue-1/lasr-2016-0008/lasr-2016-0008.pdf

designated persons and entities and the level of co-ordination and co-operation among the relevant authorities.

Materiality

24. The financial sector in Lithuania is bank-centric. According to an OECD review of the Lithuanian financial system published in November 2017, the share of the banking system in total financial system assets is 79.2 %[14]. The banking sector comprises six Lithuanian banks and seven registered branches of EU banks, mostly specialised in corporate loans, leasing or retail services. Nevertheless, the sector appears to be concentrated around three banks[15], which are all foreign-owned[16]. The banking services provided are generally traditional in nature and include loans and deposits[17]. Banks, and in particular the larger ones, have been reducing the number of their non-resident customers for de-risking purposes. The number of non-resident customers that are considered higher risk declined after the closure – in 2011 and in 2013 – of two local banks and remains very low and, by the end of 2015, the banking sector loans to non-residents amounted to 0.5 % of the total loan portfolio, and non-resident deposit to 2.5 % of the total deposits.

25. Collectively, other financial institutions (FIs) – credit unions, leasing companies, insurance companies, pension funds and capital market participants – account for less than EUR 5 billion in financial assets. The combined turnover of currency exchange offices and payment institutions does not exceed EUR 1.5 million. Electronic money institutions (EMIs) manage a negligible amount of funds.

26. The size of shadow economy in Lithuania, which is exacerbated by tax offences, constitutes a significant ML vulnerability. Thanks to aggressive nation-wide measures, shadow economy is contracting in the country but remains widespread and in the NRA it has been estimated that it amounts to 27% of the GDP. The phenomenon is associated with a very strong affinity for cash in the country and with the circulation of large amounts of cash. Financial exclusion does not appear to be an issue of major concern in Lithuania[18].

27. Money remittances play an important role in Lithuania's economy[19]. Both formal (banks, MVTS) and informal (cash couriers[20]) channels are believed to be used. In 2016 alone, the total

[14] https://www.oecd.org/finance/Lithuania-financial-markets-2017.pdf
[15] AB SEB bankas, "Swedbank" and Luminor Bank
[16] https://www.oecd.org/finance/Lithuania-financial-markets-2017.pdf
[17] The Lithuanian financial system is dominated by banks offering basic retail banking services, leasing, and insurance services. While services such as commodity derivatives are available from Lithuanian banks, retail banking services represent the bulk of their operations. https://www.oecd.org/finance/Lithuania-financial-markets-2017.pdf
[18] http://datatopics.worldbank.org/financialinclusion/country/lithuania
[19] In absolute volumes, Lithuania is in the top-five of the world's remittance recipients (3rd place in 2015 with USD 2 billion and 5th place in 2014 with 4.4% of its GDP). This is not surprising given that Lithuania has witnessed a high number of emigrants.
https://siteresources.worldbank.org/INTPROSPECTS/Resources/334934-1199807908806/4549025-1450455807487/Factbookpart1.pdf
[20] family, friends, train conductors and drivers who carry money across borders

amount of physically imported cash exceeded EUR 18 million and the total exported amount exceeded EUR 450 million[21].

28. Turning to the DNFPB sector, all types of DNFBPs operate in Lithuania, except for trustees. Company service providers (CSPs), though not subject to registration at the time of the on-site visit, are present and provide services. Thus the number of natural or legal persons providing company services is not known but the FIU believes that most of them are lawyers. However, it cannot be excluded that their services are misused in order to launder money or create fictitious companies. CSPs will be subject to registration requirements from August 2018 as a result of the 2017 AML/CFT Law which also designated the FIU as their AML/CFT supervisor. Due to the lack of awareness of ML/FT risks and to the poor implementation of (risk-based) AML/CFT requirements the DNFBP sector is considered to be vulnerable to abuse.

29. In recent years, there has been a drive by the Bank of Lithuania (BoL) to create a favourable regulatory environment for foreign Fintech companies, in order to attract foreign finance institutions and Fintech start-ups into Lithuania.[22] Another initiative to attract foreign business was launched in 2014 granting Lithuanian residence to non-EU citizens in exchange for investment.[23]

Table 1: Fintech products and services present in Lithuania

Product/Service	Licenced	Regulated	Supervised
Crowd-funding platforms	yes	yes	BoL
Peer-to-peer lending platforms	yes	yes	BoL
Consumer credit providers	Yes	Yes	BoL
Crypto-currency exchanges	No	No	No
Crypto-currency payment processors	No	No	No
Initial coin offerings (ICOs) and Token offerings	No*	Yes*	No
Blockchain-based platform for international ICO startups (Desico)	Yes**	Yes**	BoL**
Invoice finance platforms	No	No	No
Specialised banks	Yes	Yes	BoL
Payment and electronic money agencies	Yes	Yes	BoL
Blockchain protocols and platforms	No	No	No
Smart contracts	No	No	No

* Since the 8th of June 2018 Lithuania became one of the first countries in the EU to provide clarity on launching ICO projects, or sales of virtual tokens, according to a document released by the Lithuanian finance ministry.

[21] http://www.fntt.lt/data/public/uploads/2017/09/ml_tfp_activities_financial_crime_investigation_service_2016.pdf

[22] https://www.lb.lt/en/news/tags.Fintech, http://www.bankingtech.com/2018/01/lithuanias-central-bank-to-launch-blockchain-sandbox/

[23] http://www.nomoretax.eu/lithuanian-residence-in-exchange-for-investment/

** Since the 3rd of May 2018 Lithuania has introduced the world's first security ICO platform DESICO which aims to create a safe and legally regulated environment in order to develop global financial and blockchain technologies.

Structural Elements

30. The key structural elements which are necessary for an effective AML/CFT regime are generally present in Lithuania. There is a high-level commitment to address AML/CFT issues. AML/CFT policy-making and coordination is conducted through the Lithuanian FIU.

31. Lithuania is regarded as a politically-stable country. The Lithuanian legal system is principally based on the legal traditions of Continental Europe and is grounded to the principles laid down in the Constitution of the country and safeguarded by the Constitutional Court of the Republic of Lithuania.

Background and other Contextual Factors

AML/CFT strategy

32. Lithuania does not have a formal AML/CFT strategy in place. Following the completion of the NRA, the 2016-2018 Action Plan for the Mitigation of Risk of Money laundering and Terrorist Financing of the Republic of Lithuania was approved in June 2016. The action plan addresses risks that have been listed as "high-priority" in the NRA. The action plan envisages mitigation actions to be taken in four sectors: law enforcement, supervision, financial sector and non-financial sector. The coordination group discussed the results of the implementation of the Action Plan every six months and when necessary holds additional meetings. The AML/CFT Coordination makes policy proposals to the Government.

Legal & institutional framework

33. The AML/CFT legal and organisational framework in Lithuania is governed by the AML/CFT law, the Lithuanian Criminal Code (CC) as well as FIU and other governmental orders.

34. Since the last evaluation and subsequent follow-up reports, Lithuania has taken steps to improve its AML/CFT framework. Namely, following the recommendations of MONEYVAL, on 2 July 2013, the Law Amending the CC was adopted and the financing and support of terrorism has been criminalised explicitly. Financing of terrorism (FT) is now criminalised under Article 250-4 of the CC and the new criminal offence is largely conformity with the requirements of the Convention for the Suppression of the Financing of Terrorism. Another amending law of the CC was adopted in December 2013, extending the list of activities which are punishable as ML. Through these amendments, the CC appears to be in principle in line with the international requirements on the definition of ML.

35. Amendments to the AML/CFT Law were adopted in 2014[24]. The amendments reorganise the STR regime. The concept of unusual transactions has been removed. The amendments also addressed a number of deficiencies concerning customer due diligence (CDD) issues. Moreover, FIs and other entities are now required to re-evaluate the customer risk and upon the determination that they pose

[24] A new AML/CFT Law transposing the EU Directive came into force in July 2017.

a serious risk of ML/FT, apply measures of enhanced identification. Finally, the issues related to record keeping issues have been resolved.

36. The main agencies involved into Lithuania's institutional structure to implement AML/CFT regime are the following:

37. **The Money Laundering Prevention Board of the Financial Crime Investigation Service under the Ministry of Interior of the Republic of Lithuania (FIU)** is the central authority for the receipt, analysis and dissemination of information related to ML/FT. The FIU's activities are regulated in accordance with the Law on the Financial Crime Investigation Service laying down the operating principles, legal framework, objectives and functions operating controls, inter-institutional cooperation framework, powers for attorney for employees, their rights, duties, responsibilities, funding and other issues.

38. **The Prosecution Service** is a state institution performing the functions established by the Constitution of the Republic of Lithuania, the Law on Prosecution Service or other laws. The Prosecution Service organises and leads pre-trial investigations, including also with regard to ML/FT crimes, conducts pre-trial investigations in complex cases, controls activities of pre-trial investigation officers in criminal proceedings, pursues public charges in criminal cases, coordinates the acts of pre-trial investigation institutions in the investigation of criminal acts; takes part in the development and implementation of national and international crime prevention programmes, maintains international communication with foreign states and international organisations, performs other functions established by law.

39. **The Customs Department under the Ministry of Finance of the Republic of Lithuania (Customs Department)** is responsible for the controls on cash entering or leaving Lithuania. Cross-border movements of cash and bearer-negotiable instruments are regulated by the AML/CFT Law.

40. **The State Tax Inspectorate (STI)** is responsible for the administration of taxes, with the exception of customs duties. Regarding roles and responsibilities in the detection, prevention and suppression of ML/FT and PF, the STI cooperates with the Financial Crime Investigation Service (FCIS) under the Ministry of Interior (MoI) by exchanging information and providing data, including supervision of the activities of non-profit organisations (NPOs) and refers suspicious activities to the FCIS where in the course of daily duties tax officials uncover information that lead them to suspect ML/FT.

41. **The State Security Department of the Republic of Lithuania (SSD)** is an intelligence institution responsible for the prevention of terrorist financing and the coordination of counter terrorism activities, pursuant to the Law on the National Security of Lithuania. The SSD is responsible for the prevention of FT, pursuant to the AML/CFT Law.

42. **The Bank of Lithuania (BoL)** is a specialised independent institution responsible for the issuing of permits and licenses for financial market participants, monitoring their compliance – including AML/CFT obligations, and applying sanctions where breaches are identified.

43. **The Department of Cultural Heritage under the Ministry of Culture** supervises persons (both individuals and legal entities) trading in movable cultural properties and/or antiques in general. Where the value of these objects exceeds EUR 15,000 to the extent that payments are made in cash, it informs the FIU. The very recent change was made by adopting a new Controlling questionnaire No Į-235 for trading antiques on 30 October 2017.

44. **The Gaming Control Authority (GCA)** is responsible for the licensing and AML/CFT supervision of land-based casinos and online casinos.

45. **The Lithuania Chamber of Notaries** is a self-governing body of notaries. Every notary is a member of the Chamber of Notaries. According to Article 30 of the AML/CFT Law, the Lithuanian Chamber of Notaries is the supervisory authority for notaries.

46. **The Lithuanian Chamber of Auditors** is responsible for the supervision of of auditors regarding the implementation of AML/CFT provisions.

47. **The Lithuanian Assay Office (LAO)** oversees the activities performed by economic operators in the field of precious metals and gems. According to AML/CFT law of the Republic of Lithuania, the LAO is responsible for the AML/CFT supervision traders in precious metals and gems.

48. **The Lithuanian Bar Association** supervises the activities of advocates and advocates' assistants related to the implementation of AML/CFT measures. The Lithuanian Bar Association is a public legal entity, representing the interests of advocates and advocates' assistants in public institutions, international and foreign organisations. As a self-regulatory institution of advocates, it is responsible for the prevention of ML/FT. Its main roles include approval of instructions aimed at preventing ML/FT intended for advocates and advocates' assistants; supervision of activities of advocates and advocates' assistants related to the implementation of AML/CFT measures; advising advocates and advocates' assistants on the issues relating to the implementation of the instructions.

49. **The Centre of Registers** is responsible for the administration of five main state registers. It also manages its own certification authority – the Certification Centre of the Centre of Registers. The Register of Legal Entities (RLE) – one of the state registers administered by the Centre – registers businesses, institutions and NGOs and collects detailed data about Lithuanian legal entities as well as branches and representative offices of foreign companies and organisations.

Financial sector and DNFBPs

50. The Lithuanian banking system dominates the country's financial sector. As of November 20, 2017, six national banks and seven branches of foreign banks were registered in the register of the Bank of Lithuania. The total value of banking assets was estimated at EUR 25.762,9 million in November 2017.

Table 2: Licensed Banks by the BoL

Bank Name	**Bank Asset (mln. EUR)**
Medicinos Bank	265,9
Citadele Bank	503,6
šiauliu Bank	1823,6
DNB	3995,4
Swedbank	7326,8
SEB	7524,1
7 foreign bank branches	4323,5
Total:	25762,9

51. As of 31 September 2017, the total assets of credit unions amounted to EUR 666.352,6 million, the total assets of insurance companies amounted to EUR 246.721,9 million.

52. As of 31 September 2017, no statistics were available on the activities of EMIs, especially because not all the 27 registered ones have been carrying out activities.

53. As of 20 November 2017, the following non-bank FIs were subject to the supervision of the BoL:

Table 3: Number of Non-bank Financial Institutions

Type of Entity	No. Licensed/Regulated/Registered
Insurance Companies	8[25]
Credit Unions	70+1[26]
Electronic Money Institutions	27[27]
Payment Institutions	43[28]
Financial Brokerage Companies	7
Currency Exchange Operators	23
Management Companies	24
Investment Companies	31
Peer-to-peer Lending Platform Operators	7
Crowd Funding Platform Operators	5

54. As of 31 December 2017, the following DNFPBs were subject to the licensing and supervisory Authorities indicated in the next table:

Table 4: Number of DNFBPs

Type of Entity	No. Licensed/Regulated/Registered
Real estate agents	Unknown
Dealers Precious Metals and Stones	1,777
Lawyers, including judicial officers	3,603
Notaries	262
Accountants and Auditors	352
Licensed antique merchandisers	72
Casinos (land-based and internet based only)	25

Table 5: Licensing and Supervisory Authorities of DNFBPs

DNFBPs	Licensing Authority	AML/CFT Supervisor
Real estate agents	Center of registers	FIU
Dealers in precious metals and precious stones	Lithuanian Assay Office	Lithuanian Assay Office
Lawyers	Lithuania Bar Association	Lithuania Bar Association
Other independent legal professionals	Lithuania Bar Association	Lithuania Bar Association
Lawyers and other independent legal professionals	Lithuania Bar Association	Lithuania Bar Association
Notaries	Ministry of Justice	Chamber of Notaries
Accountants	No information provided	FIU
Auditors, audit firms	Chamber of Auditors	Chamber of Auditors

[25] This included 5 life insurance companies and 3 branches of life insurance companies.
[26] 1 Central Credit Union.
[27] This included 20 electronic money institutions with full operating license and 6 electronic money institutions with limited operating license.
[28] This included 30 payment institutions with full operating license, 12 payment institutions with limited operating license and 1 branch of a payment institution.

Trust and Company Service Providers	Centre of registers	FIU
Casinos	Gaming Control Authority	Gaming Control Authority

Preventive measures

55. The cornerstone of the AML/CFT preventive measures is the AML/CFT Law. The Law was adopted in June 1997 and amended several times. The most recent amendments, dating back the 13th of July 2017, have been adopted taking into account the provisions of the Directive of the European Parliament and Council (EU) 2015/849 and FATF standards. The aim of such amendments was to change and supplement the already existing AML/CFT Law.

56. After the entry into force of the consolidated version of the AML/CFT Law, the number of actors subjected to the law has been widened. The provisions of the new regulation are applicable to all the persons involved in commercial activities – including trade in immovable objects, gems, precious metals, antiques, etc. – whose price exceeds EUR 10,000 or the corresponding amount in foreign currency and when the payment is made in cash, to all the actors involved in the arrangement of gambling and lottery activities and to the agents of immovable property.

57. The new amendments specify a number of issues. Among others, the requirements for the identification of the client and the beneficial owner (BO). Moreover, the new version of the AML/CFT Law provides that the NRA on ML/FT should be effectuated every four years. The NRA – together with the conclusions of the European Commission (EC) – will have to be taken into account by FIs and the other entities when defining their control procedures of the internal policies and internal controls.

58. For the violations in the implementation of the AML/CFT preventive measures, the AML/CFT Law put in place an effective, proportional and deterring system of sanctions. The wide range of sanctions foreseen by the AML/CFT Law allows the supervising authorities to take into due account the differences related to size, features and characteristics of the activities of the FIs and other entities involved. The supervision of the provisions contained in the AML/CFT Law is performed by the BoL, the FCIS, the GCA, the Department of Cultural Heritage, the LAO, the Chamber of Auditors of Lithuania, Lithuanian Bar Association, the Chamber of Notaries of Lithuania and the Chamber of Bailiffs.

Legal persons and arrangements

59. The main law governing the creation and regulation of legal persons in Lithuania is the Lithuanian Civil Code. Article 2.62 of the Civil Code is the provision that regulates the different types, forms and basic features of legal persons in the country. Detailed and publicly available information on the creation and types of legal persons is available on the website of the RLE, in the website of the STI, in the website of Enterprise Lithuania, in the website of the Ministry of Economy (MoE), in private companies and law firms.

60. All legal entities of different legal forms have to be registered in the RLE. According to Article 2.71 of the Civil Code "Register of Legal Persons", all the documents and the information supplied to the register shall made public. Every person shall have the right to receive, free of charge, oral information on the legal status of a legal person and restrictions imposed of his activities in accordance with the procedures established by the RLE.

61. The Information System of Members of Legal Persons (JADIS) started to operate on 1 August 2014. According to Article 25 of the new version of the AML/CFT Law (and to Articles 2.66 and 2.71 of the Civil Code), all legal entities – with the exception of the ones whose sole shareholder is the State or a Municipality – receive, update and store detailed information to the Information System no later than ten days after the exchange of data. All the data collected and submitted to the Information System of Members of Legal Entities are not public. They are available for authorised users and for state authorities and institutions in order for them to perform their duties. Other interested natural or legal persons can receive extracts of legal persons' basic information contained in JADIS against a fee.

62. As of 31 December 2017, the types of legal persons present in Lithuania were:

Table 6: Number of Legal Persons (including branches and representation offices)

Type of Entity	No. Registered
State-Owned Enterprise	79
Branch of State-Owned Enterprise	36
Representative Office of State-Owned Enterprise	0
Municipal Enterprise	39
Branch of Municipal Enterprise	0
True Partnership	232
Branch of True Partnership	4
Partnership	152
Branch of Partnership	4
Gardeners Community	1,384
Community	9,149
Private Company Limited by Shares	124,122
Branch of Private Company Limited by Shares	1,021
Representative Office of Private Company Limited by Shares	18
Public Limited Liability Companies	372
Branch of Public Limited Liability Companies	126
Agricultural Company	1,006
Branch of Agricultural Company	3
Permanent Commercial Arbitration Body	7
Branch of Foreign Legal Entity and Other Organisation	621
Representative Office of Foreign Legal Entity or Other organisation	873
Credit Union	1
Public Institution	10,554
Branch of Public Institution	177
Representative Office of Public Institution	1
Chamber of Commerce, Industry and Crafts	5
Branch of Chamber of Commerce, Industry and Crafts	5
Association	18,948
Branch of Association	199
Representative Office of Association	10

Charity and Support Foundation	1,623
Branch of Charity and Support Foundation	15
Representative Office of Charity and Support Foundation	2
Political Party	28
Branch of Political Party	26
Religious Community or Society	190
Traditional Religious Community or Society	1,114
Cooperative Company (Cooperative)	651
Branch of Cooperative	4
Household	58
Trade Union or Association	1,786
Branch of Trade Union	79
Individual Enterprise	37,270
Branch of Individual Enterprise	436
Lawyers Union	103
European Economic Interest Grouping	3
European Company	1
Central Bank	1
Association of Lithuanian Chambers of Commerce, Industry and Crafts	1
General Management and Notification Centre	1
Budget Institution	3,250
Branch of Budget Institution	708
Small Community	11,897
Branch of Small Community	2
Total:	**228,397**

Supervisory arrangements

63. The BoL is responsible for the authorisation, regulation and supervision of all FIs. The BoL, in performing its duties, operates under the AML/CFT Law and under the Law on the Bank of the Republic of Lithuania. Under the currently existing risk-based supervision model of the BoL, the supervision of AML/CFT requirements is allocated to the Supervisory Services Prudential Risk Supervision Department Operational Risk Division. The general risk-based supervision policy is stated in the BoL Financial Market Supervision Policy and the Risk-Based System Concept of the BoL Supervisory Services. Main AML/CFT supervisory principles are set in the Operational Risk Supervision document.

64. On-site visits and off-site supervisory actions are the mean ways through which supervision is carried out. Off-site supervision is based on regular reports from all supervised entities (including but not limiting banks and insurance companies). Data is being acquired on the basis of the questionnaire (quantitative and qualitative non-structured data reporting) which is updated on a yearly basis as well as the received quarterly compliance, risk and internal audit reports from the banks, major bank branched and Central Credit Union. Moreover, information about companies received during licensing process, relevant information from other sources such as NRA,

Supranational Risk Assessment and media can be used for determining FI's ML/FT risk level and frequency and intensity of on-site and off-site supervisory actions.

65. Different supervisory bodies are responsible for the AML/CFT supervision of DNFBPs. The GCA exercises supervision over casinos and organisers of games of chance. The Lithuanian Chamber of Notaries is responsible for the supervision of Notaries. The Chamber of Auditors supervises auditors. The Chamber of Judicial Officers of Lithuania is in charge of the supervision of judicial officers and judicial officers' agents. The LAO supervises persons engaged in economic and commercial activities related to trading in precious stones and/or metals. The FCIS exercises supervision on all categories of DNFBPs.

International Cooperation

66. Lithuania has a sound legal and procedural framework to exchange information and cooperate with its foreign counterparts in relation to ML, associated predicate offences and FT. In general, cooperation among Lithuania and the other Baltic countries is well developed, and information exchange with other EU Members takes place on a daily basis. Regular cooperation based on UN instruments and bilateral agreements with non-EU countries has been noted, in particular with regard to neighbouring countries. The authorities of Lithuania take active part in the work of multilateral fora, both at policy and at the operational level, as MONEYVAL, Interpol, Europol or Eurojust. Lithuania has signed and ratified the relevant international treaties regulating cooperation, and taken steps into the UNSCRs in areas relevant to AML/CFT.

CHAPTER 2. NATIONAL AML/CFT POLICIES AND COORDINATION

Key Findings and Recommended Actions

Key Findings

1. Lithuania's understanding of ML/FT risks is largely based on the NRA completed in 2015. The NRA focuses on threats and vulnerabilities and does not consider the resulting risks. As a result, while the authorities may be in a position to know which illicit activities generate proceeds of crime and which areas may be vulnerable to misuse, they do not have a full understanding of how money is being laundered in the country or whether FT is taking place.

2. Other factors concerning the NRA militate against a full understanding of risk: the NRA does not provide a description of the main ML methods, trends and typologies; it is not based on a sufficiently wide array of information sources; the involvement of supervisory authorities, particularly the BoL, was limited and some not involved at all - the judiciary; it does not contain a large degree of granularity - for instance, there is no assessment of the products, services and customers that pose a higher risk; cross-border threats are not considered; certain risks, including the use of fictitious companies, risks in the Fintech sector, and the use of cash, have not received any significant attention.

3. The understanding of FT risk evolved following the completion of the NRA. The law enforcement community, particularly the SSD, displayed a more sophisticated knowledge of the risk. However, this understanding has not been communicated to other authorities and the private sector. There are areas of ineffective application of the Standards, such as weak controls at the borders, that further reduce opportunities to understand the risk.

4. Lithuania completed an action plan in 2017 to address a number of threats and vulnerabilities identified in the NRA. Concrete results have already been achieved, such as for instance the reduction of tax evasion and the shadow economy, which are considered to increase the risk of ML. However, despite the completion of the action plan, further efforts are needed to mitigate significant vulnerabilities, such as the investigation and prosecution of ML and AML/CFT supervision. Weak controls at the border remain unaddressed and pose a significant vulnerability.

5. Lithuania does not exempt FIs and DNFBPs from AML/CFT obligations. Enhanced due diligence (EDD) measures are required based on, *inter alia*, legal requirements, the internal policies and procedures of private sector entities and the results of the NRA. It is doubtful whether the NRA provides a useful basis to support the application of EDD. Simplified due diligence (SDD) measures are permitted. The lower risk scenarios are not inconsistent with the NRA, although this is not unexpected given the lack of granularity of the NRA.

6. The objectives and activities of the law enforcement community and the Prosecution Service have long been evolving to target the most serious threats, including organised crime, corruption and financial crime. ML related to such crimes has started receiving significant attention closer to the date of the evaluation. The objective and activities of supervisory authorities have started developing in line with risks, although it is too early to measure the success of the actions being taken.

7. Lithuania has a strong co-ordination mechanism in place. The AML/CFT Coordination Group serves as a national body to develop policy and co-ordinate actions at a national level. Operationally, there are many agreements in place between the different authorities to ensure the smooth and efficient exchange of information.

8. There are no formal mechanisms in place to co-ordinate actions for PF.

9. The results of the NRA were communicated to all private sector entities through various means. While banks and other FIs were aware of the content of the NRA, this was to a lesser extent the case in relation to DNFBPs.

Recommended Actions

1. Lithuania should, as a matter of priority, conduct the next iteration of the NRA, which should:

a) involve supervisory authorities, especially the BoL, more directly – for instance all supervisory authorities should be involved in the discussions of working groups set up to discuss threats and vulnerabilities and not just be required to complete questionnaires;

b) be based on a more comprehensive set of qualitative and quantitative information sources – for instance, information from the SSD on FT risks, information from the BoL on the risks posed by cash and non-resident customers, information from the FIU on typologies and more detailed statistics;

c) consider to a larger degree the cross-border ML threat (at least include an assessment of: financial flows to and from high risk countries, MLA requests received and sent, international informal requests from and to FIU and LEA, STRs and cash declarations), the use of fictitious companies (by analysing information from LEAs), the use of cash (by analysing information from the FIU, the BoL, the Customs Department and the STI);

d) involve a more targeted assessment of the ML/TF risks arising from the use of cash in the country. In particular, Lithuania should consider how different vulnerabilities related to use of cash have been

or may be potentially exploited by the threats in order to determine the manner in which ML/TF risks have materialized;

e) assess the vulnerabilities of the Fintech sector;

f) for the purpose of the assessment of FT risks, separately consider the risks of movement, collection, provision and use of funds and include an assessment of the vulnerabilities of financial instruments and risks related to flows to high-risk jurisdictions.

2. Information on FT risks should be shared among all competent authorities and the private sector, as appropriate, to permit a fuller and more rounded understanding.

3. Depending on the risks identified through an updated NRA, identify, apply and monitor the application of suitable mitigating measures.

4. Based on the results of the next iteration of the NRA, all supervisory authorities should issue guidelines on the application of EDD measures by the private sector.

5. Establish mechanisms for the co-ordination of PF actions. The authorities may wish to extend the mandate of the AML/CFT Coordination Group to cover PF issues and the membership of the Group to include other relevant stakeholders, such as the MoE.

6. Strengthen communication mechanism of NRA results to DNFBPs.

7. Statistics should be maintained in relation to a more comprehensive set of data (e.g. MLA requests).

Immediate Outcome 1 (Risk, Policy and Coordination)

Country's understanding of its ML/TF risks

67. The authorities' understanding of ML/FT risks derives primarily from a NRA completed in 2015, which saw the involvement of various competent authorities and some private sector entities, mainly banks. There is broad consensus among the authorities on the conclusions of the NRA and the rating assigned to the various threats and vulnerabilities. However, there are a number of factors which impinge upon the adequacy of the NRA as a result of which the understanding of risk in Lithuania is rather high-level in nature.

68. The NRA identifies a list of ML/FT threats and vulnerabilities. For instance, organised criminality (involving drug trafficking, fraud and smuggling of goods), tax evasion, fraud and corruption are considered to be the highest ML threats. Lack of supervision (including lack of resources of supervisors, supervisory activities and imposition of sanctions), high circulation of cash, the shadow economy and shortcomings in the application of preventive measures by DNFBPs (including inability to monitor transactions and verify beneficial ownership) are identified as major ML/FT vulnerabilities. The NRA does not consider how the different vulnerabilities have been or may be potentially exploited by the threats in order to determine the manner in which ML/FT has materialised and which areas may be at an elevated risk.

69. Linked to the foregoing, but also as a separate concern, the NRA does not provide a detailed picture of the main methods, trends and typologies used to launder proceeds of crime in Lithuania. The authorities may be in a position to know which illicit activities are generating proceeds of crime, which areas within the country are vulnerable to abuse and those parts of the national AML/CFT

system which are not functioning effectively, but they do not have a full understanding of how money is being laundered in the country or whether terrorism financing is taking place. For this reason, the assessment team considers that the NRA is of somewhat limited use to the authorities when implementing mitigating measures and to the private sector, which is required to take into consideration the results of the NRA in establishing internal controls. This has been confirmed by the majority of private sector entities met on-site.

70. There are other issues which support the above conclusions. For instance, there is no assessment of the types of products and services within the financial sector that have been or may be misused for ML/FT purposes. The NRA simply identifies the use of technology in money transfers as a high-risk priority area within the financial sector, without specifying either which technologies are particularly risky or the scale of the problem. Similarly, the ineffective application of preventive measures by DNFBPs is considered as a risk. However, there is no indication of which part of, or the extent to which, the DNFBP sector has been misused for ML or FT purposes. The same could be said of the widespread use of cash in Lithuania, which is listed as a higher risk without articulating the manner in which cash has been exploited by criminals to launder money or finance terrorism. The understanding of the degree to which cash may be used for ML or FT purposes may also be limited due to ineffective measures at the border to detect undeclared and falsely declared cash.

71. The level of cross-border illicit flows does not appear to be addressed to any degree in the NRA. Although the assessment team has not concluded that this poses a major risk, there have been several ML convictions which contained a cross-border element. On-going investigations involving foreign proceeds of crime were also referred to by LEAs and the FIU during the on-site visit. Additionally, organised criminal groups in Lithuania maintain close links with criminal groups in neighbouring countries. The assessment team would have expected the NRA process to include, at a minimum, a comprehensive analysis of: (1) financial flows with higher risk countries, (2) mutual legal assistance (MLA) requests received and sent in relation to ML and other proceeds generating crimes (3) FIU requests for information with foreign counterparts and (4) STRs involving foreign persons[29] and or cross-border transactions to determine Lithuania's level of exposure to foreign ML/FT threats.

72. Some other ML-related risks have not received sufficient attention during the NRA process. Weaknesses in the cash declaration system are not included as a vulnerability. Despite the fact that there has been a drive by Lithuania to create a favourable regulatory environment for foreign Fintech companies, no risk assessment has been carried out.

73. In general, the ML/FT risks associated with legal persons have not been assessed in a meaningful manner, except for weaknesses in the identification of beneficial ownership identified as a vulnerability in the NRA. However, the authorities understand that the use of fictitious companies in criminal schemes poses a significant risk. Further information is provided under core issue 5.2.

74. Another limiting factor is the fact that the NRA is not grounded in a sufficiently comprehensive set of information, either quantitative or qualitative. This is partly due to the absence of some key datasets (e.g. statistics on MLA), but also the failure to feed certain critical information into the risk assessment process (e.g. information from the SSD on FT risks) and the limited involvement of supervisory authorities, especially the BoL. The judiciary was not involved at all.

75. Despite the various shortcomings identified in relation to the NRA, the understanding of certain ML risks at institutional level is more developed. For instance, the BoL has conducted various

[29] Although this has been considered by the FIU in its annual reports

thematic reviews of risks within the banking sector in relation to the use of cash and non-resident business. The FIU conducts typology exercises periodically. The Criminal Police Bureau conducts threat assessments of organised criminality on a yearly basis. The assessment team has considered these initiatives closely and found them to be very adequate. It is suggested that for the next iteration of the NRA, Lithuania incorporates all of this information to obtain a more rounded view of ML risks.

76. The assessment of FT risks in the NRA is largely based on hypothetical scenarios. The law enforcement community, especially the SSD, displayed a more sophisticated knowledge of these risks as indicated under IO 9. This understanding has not been communicated to other authorities and the private sector. There are areas of ineffective application of the Standards which militate against a full understanding of FT risks, such as weak controls of cash transportation at the borders and inadequate application of preventive measures by certain MVTS providers.

National policies to address identified ML/TF risks

77. Lithuania established an action plan in June 2016 to address the threats and vulnerabilities identified in the NRA. Most actions had been completed by the time of the on-site visit. Although, as noted in core issue 1.1, the assessment team considers that Lithuania, through the NRA, has not identified certain risks and certain risks are not understood to a significant extent, under this core issue the assessment team focuses on, and gives credit to Lithuania for, some mitigating measures implemented in relation to threats and vulnerabilities that were actually identified.

78. One area which received very close cross-institutional attention, separately from but also as part of the NRA action plan, was the shadow economy, particularly aspects related to the evasion of tax and the use of cash, all of which are considered to significantly increase ML risks. On tax evasion, the STI implements and periodically updates a consolidated action plan to ensure taxpayer compliance. This includes measures mitigate risks in the most risky economic sectors, such as construction and catering services. Measures were implemented to limit the ability of tax payers to settle transactions in cash in a number of scenarios (restricting the use of cash for payments when there is a reasonable risk that a taxpayer paying in cash can hide income or in other ways avoid to pay taxes, requiring loan agreements in cash exceeding a certain limit to be notarised, etc.), education and awareness-raising strategies, making data about taxpayers publicly available and sharing of information between the FCIS/SSD and the STI on taxpayers. Many of these measures have been implemented successfully, such that a noticeable reduction in the shadow economy has been registered. It was mentioned, for instance, that the VAT gap reduced from 30.7% in 2012 to 24% in 2016.

79. As part of the NRA action plan, the BoL carried out a ML risk assessment on the use of cash in banks, which was completed and presented to the banks in 2016. A number of shortcomings were identified, which banks were required to rectify. This has also prompted the BoL to include a number of questions on cash transactions in its offsite inspection programme. Other mitigating measures include: special attention to cash related businesses and transactions during the on-site inspection process and data on cash transactions in annual AML/CFT questionnaires which is used for constant monitoring. As a result of increased attention by the BoL to cash controls, the majority of banks lowered the threshold for currency exchange transactions (e.g. starting from 1 euro). Following the completion of the NRA, a decision was made to lower the currency exchange transaction threshold (since 13 July 2017, when exchanging cash FIs are required to identify and verify the customer and the beneficial owner when the transaction is equal or exceeds EUR 3,000 (instead of EUR 6,000), an

initiative which was supported by the BoL. There is a cash-transaction reporting requirement, which is effectively applied and provides an additional information resource to the FIU. The authorities have also taken measures to increase the visibility of notifications concerning the declaration of cash at the borders, conducted awareness raising events for businesses regarding cash declaration requirements and training activities for Customs officers. It should be noted that serious concerns remain about the ability of the Customs Criminal Service of the Customs Department to detect suspicious cash at the border as noted under IOs 6, 7 and 8.

80. Mitigating measures against the use of fictitious companies were taken, as explained under core issue 5.3 of this MER.

81. Organised criminality is listed as the most serious ML threat in the NRA and was placed at the top of law enforcement priorities under the action plan. In pursuance of this objective, training was provided to 189 prosecutors and 208 investigators over a period of two years (2016-2017). The training, entitled 'Methodology for Investigation of Criminal Offences Committed by Organised Crime Groups', focuses specifically on the techniques required to pursue crimes committed by organised groups, including through asset deprivation, and to dismantle such groups. In addition, a structured methodology-based model for serious and organised crime threat assessment was implemented to monitor, analyse, control and improve the crime-related situation in Lithuania. This has already had tangible effects, as demonstrated by cases presented under IO 7.

82. Measures have also been implemented to tackle corruption, one of the highest four ML threats. The strategy is based on an inter-institutional action plan, which is part of a national anti-corruption programme adopted in 2015. The action plan includes measures such as the carrying out of corruption risk analyses related to state or municipal institutions, assessments of legal acts on anti-corruption and information on persons seeking or holding office in state or municipal institutions. All of these measures are conducted on an on-going basis. The authorities provided many examples of how these measures have been implemented, which in the interest of brevity cannot be listed. Just as an example, the SIS carried out 20 corruption risk analysis and submitted 841 recommendations in 2017 to the Government. 84% of the recommendations had been implemented at the time of the on-site. For instance, based on these recommendations, the Parliament adopted a legal act No. 533 (dated 28 of June, 2017) which regulates the procedures of providing financial support by state owned enterprises.

83. In relation to FT risks, the FIU conducted an analysis of transactions carried out by a segment of the NPO sector to determine whether any suspicions should be flagged with the SSD for further action. FIU products were disseminated to the SSD, which found that no further action was required. The list of criteria for reporting STRs available to the private sector was updated by the FIU to include indicators related to the abuse of NPOs for FT purposes. The banking sector closely monitors the activity of NPOs and applies enhanced measures to transactions flowing to high-risk jurisdictions. The BoL obtains information on the latter in particular from its onsite and off-site supervision. While positively noting these initiatives, it is the view of the assessment team that further measures should be taken to address FT risks, as noted under IO 9 and 10.

84. Some efforts were made to address two overarching vulnerabilities of the national AML/CFT system; the ineffective identification, investigation and prosecution of ML and shortcomings in the supervision of both the financial and non-financial sectors. Training was provided to prosecutors and investigators on financial investigations. However, more progress is needed in this area, since as noted under IO 6, 7 and 8, the results both in terms of ML convictions and confiscation of proceeds of

crime remain very modest. Most supervisors are in the process of strengthening their supervisory measures, including through the implementation of a risk-based model.

Exemptions, enhanced and simplified measures

85. There are no exemptions in relation to the FATF's descriptions of types of financial institution and DNFBP which should be subject to AML/CFT obligations.

86. Under Article 14 of the AML/CFT Law, obliged entities are required to perform enhanced due diligence (EDD) in relation to cross-border correspondent banking relationships, PEPs and transactions or business relationships with natural persons residing or legal persons established in high-risk third countries. EDD must also be performed in cases indicated by the European Supervisory Authorities (ESAs) and the EC and where a higher risk of ML/FT is identified based on the risk assessment and management procedures established by the obliged entities. The same article lists the additional measures to be applied in cases where EDD is required. Article 26 of the AML/CFT Law requires the NRA to be taken into account in order to apply measures in line with the level of risk identified and in certain cases adjust the measures to be taken. Because of the limitations of the NRA as noted under core issue 1.1, it is doubtful whether the results of the NRA provide a useful basis to support the application of EDD by the private sector. Moreover, none of the supervisory authorities have issued any guidance on the application of EDD.

87. Simplified due diligence (SDD) may be carried out in situations listed under Article 15 of the AML/CFT Law where lower risk of ML/FT is identified based on the risk assessment and management procedures established by the obliged entities. SDD can be applied, under limited conditions, to specific types of customers (designated listed companies, entities of public administration, financial institutions) or products (designated life insurance contracts, pension schemes, electronic money in case of an annual turnover which does not exceed EUR 1,000, lotteries and deposits accepted from natural persons) and in cases indicated by the ESAs and the EC. The same article also refers to the measures that obliged entities may derogate from when applying SDD and situations in which the application of SDD must cease or should not be applied. While the provisions under Article 15 of the AML/CFT Law do not appear to be unreasonable, there was no analysis which would support the application of SDD[30]. Nevertheless, the lower-risk scenarios are not inconsistent with the NRA, although this is not unexpected given the lack of granularity of the NRA.

Objectives and activities of competent authorities

88. The activities of the prosecution and LEAs are governed by the Long-Term Strategic Action Plan of the Prosecution Service of the Republic of Lithuania for 2013-2023. Although it was adopted prior to the completion of the NRA, it covers the ML and FT threats identified therein and is sufficiently dynamic and flexible to allow the prosecution and LEAs to adapt their objectives and activities in line with new and emerging risks.

89. The priorities of the action plan are the combatting of economic and financial crimes (which include both ML and FT), corruption and organised criminality. Economic and financial crimes and corruption are pursued by two specialised bodies, the FCIS and SIS, which were specifically set up for

[30] The authorities point out that SDD is prohibited if obliged entities cannot prove low risk of ML/TF (SDD may only be applied if the risk assessment conducted by the obliged entity can prove that the risk of ML/TF is low; risk shall be monitored constantly.

that purpose. In the view of the assessment team this is a prime example of how law enforcement resources should be allocated to areas which pose significant risk, both in terms of human resources and expertise. Lithuania should be commended for this. In addition, the prosecutorial supervision of economic and financial crime was elevated to more senior levels due to the complexity that investigations of these types of crimes may involve.

90. While there is no specialised function for ML, prosecutors have been appointed within the Department for Criminal Prosecution of the Prosecutor General's Office and specialised divisions of regional prosecutors' offices to specialise in the fields of ML and unjust enrichment. Similarly, prosecutors have been appointed within the Departments Organised Crime and Corruption Offices at central and regional level to specialise on FT. The Prosecutor General issued binding recommendations on financial investigations and training in this area was intensified to increase the effectiveness of the framework for the seizure and confiscation of proceeds of crime, especially in relation to organised criminality, corruption and economic and financial crime. While the objectives and activities of the prosecution service and law enforcement have clearly evolved to target the most serious proceeds-generating crimes, ML related to these crimes has not been targeted as aggressively.

91. One area which has remained stagnant despite existing and evolving risks is the control of cash at the borders. The Customs Department has not made significant progress since the previous evaluation in the detection and restraint of cash transported to and from Lithuania.

92. The BoL has demonstrated strong commitment during the last two years in particular to increasing its resource capacity so as to continue to move towards comprehensive risk-based supervision. While it has had resource issues, its staff has been proactive both in identifying and assessing risk and in addressing it. The BoL's objectives and activities are aligned with national policies. The alignment of the objectives and activities of DNFBP supervisory authorities varies but the FIU and the Gaming Control Authority, while some way short of risk-based supervision, have demonstrated that their approaches align with those nationally.

National coordination and cooperation

93. The AML/CFT Coordination Group was set up by Order No 154 of the Prime Minister of 2 May 2013 and started functioning in June 2013. The Group is headed by the Vice Minister of the Interior and comprises high-ranking officers from all AML/CFT competent authorities. The decisions of the Group are recorded after each meeting and must be executed by designated institutions. The Group is a policy-making body, which deals with all the issues related AML/CFT.

94. Order 154 sets out three main functions of the Group: (1) to coordinate cooperation of state authorities, financial institutions and other entities in the prevention of ML/FT; (2) to make suggestions regarding the improvement of the ML/FT prevention system; (3) to prepare proposals for improvement of relevant acts and to present them to relevant state authorities.

95. From a review of the minutes of the meetings of the Group it transpired that during the period under review, the Group discussed various shortcomings and made proposals to change the AML/CFT Law and other legislative acts. The NRA process, which started in the summer of 2014, was overseen by the Group, which also approved the Action Plan for the Risk Mitigation of ML/FT 2016-2018. Although no AML/CFT national strategy exists in Lithuania, discussions at the Group are generally aimed at setting priorities and influencing government policy on AML/CFT matters.

96. Outside of the Group, cooperation between the different AML/CFT supervisory authorities takes place through the FIU, which has signed MoUs with all the authorities included in the AML/CFT Law. The FIU has a supervisory role and has the power to coordinate the activities of the institutions involved in the implementation of ML/FT prevention measures. Cooperation between the FIU and the supervisory authorities takes the form of intelligence exchanges (for instance, in the course of licensing of FIs), discussions on risks, training of REs and conducting joint on-site inspections. The level of cooperation between the FIU and the various supervisory authorities appears to be adequate, in particular with the BoL.

97. The BoL and the Police meet periodically to discuss patterns of crime which may affect the financial sector. This also happens, albeit to a lesser extent, with the Ministry of Finance (MoF) and the Ministry of Foreign Affairs (MFA). It is less clear if cooperation and sharing of information exists between the various supervisory authorities aside from the discussions that are conducted within the Group.

98. The Collegiate Council of the Prosecutor's Office plays a determining role in implementing national policies and co-ordination of prosecutorial and law enforcement action. Since 2017, the Prosecutor General's Office (PGO) has been approving the action plans related to the implementation of the Long Term Strategic Plan. Prosecutors' Departments and Offices are required to report periodically on the implementation of plan indicators. This has the effect of ensuring that the goals of the Strategic Plan are achieved in a coordinated manner. At a more operational level, it was clear from the on-site interviews that there is constant and smooth cooperation between the various LEAs without any practical or statutory impediments. A database of criminal intelligence investigations has been developed to enable different LEAs to cooperate on the same case and avoid duplication of investigative actions. LEAs also cooperate with the FIU. During 2017, according to the authorities, the FIU received close to 900 requests from different LEAs. Two chief investigators at the FIU were designated to respond to requests.

99. On 7 May 2015, the Seimas of the Republic of Lithuania adopted the Public Security Development Programme for 2015-2025, whose aim is to ensure that Lithuania becomes a more secure state capable of effectively protecting fundamental human rights and freedoms and public security. The third goal of the programme relates to terrorism and FT. With a view to implementing this goal, the SSD established a working group which is aimed at dealing with issues related to the fight against terrorism and FT. The following institutions are involved in the activities of this group: the SSD, the Ministry of Interior, the Police, the FCIS, the VIP Protection Department, the State Border Guard Service, the PGO, the Ministry of Foreign Affairs, the Ministry of Justice, the Ministry of Culture, the Ministry of Social Security and Labour, the Ministry of Health and the Joint Staff of the Armed Forces of Lithuania. In October 2016, the first meeting of the CT working group took place. The members discussed a proposal drawn up by the SSD with regard to an action plan aimed at implementing the tasks of the Public Security Development Programme. This action plan was approved in the group meeting which took place in December 2016. In response to various terrorist attacks in EU Member States, the SSD organised various meetings of the CT working group to discuss terrorism and FT prevention. The participants discussed actions to be taken in order to prevent any possible expansion of the terrorism threat in Lithuania.

100. There is no national mechanism for coordination and implementation of policies and strategies to counter PF in Lithuania, although relevant issues are included in the weekly agenda of the CoM of Lithuania. The MFA as a coordinating authority in the PF area has developed a good level of

cooperation with the MoE, the Customs Department and the SSD when it comes to the licencing and authorisation of strategic and dual use goods.

Private sector's awareness of risks

101. The NRA report was published in 2015 and is easily accessible on the website of the FCIS. Upon publication, the report was circulated to all the authorities involved in the process, members of the AML/CFT Coordination Working Group, and simultaneously conveyed to the public through a press release. The FIU circulated the NRA by email to all FIs and all regulatory authorities/associations of DNFBPs. Conferences and seminars were organised by the FIU and some supervisors and SRBs in order to present the content of the report to the obliged entities and their members.

102. While all banks and most of the other FIs met on-site were aware of the content of the NRA, this was to a lesser extent the case in relation to DNFBPs. Some, such as for instance tax advisors and real estate agents, were completely unaware of the existence of the report. The NPO representatives were not aware of the NRA either. In most cases, private sector entities agreed that the document was useful in presenting a comprehensive picture of the ML/FT threats and vulnerabilities in the country. However, in their view, the results of the assessment did not provide practitioners with a clear orientation of the risks present in the country and the features of their business areas which presented a higher risk.

Conclusion

103. **Lithuania has achieved a moderate level of effectiveness for IO 1.**

CHAPTER 3. LEGAL SYSTEM AND OPERATIONAL ISSUES

Key Findings and Recommended Actions

Key Findings

Immediate Outcome 6

1. LEAs are active in generating financial intelligence through the application of the Law on Criminal Intelligence (LCI), which has as one of its objectives the search for criminal proceeds, and the PG's Recommendations on Financial Investigations, which requires the conduct of financial investigations during criminal intelligence investigations of proceeds-generating crimes.

2. Financial intelligence, generated on the basis of the LCI and the PG's Recommendations, has been successfully used by LEAs to determine whether the suspect is in a position to prove that the income sources are lawful or whether the suspect has failed to declare income to the STI. However, financial intelligence has not been extensively used to follow the trail of proceeds of crime to establish new or additional links within an investigation of predicate offences. Consequently, such intelligence has not been widely used to develop evidence related to ML (or FT).

3. The FIU has broad and unhindered access to information sources to develop financial intelligence and makes use of these sources on an on-going basis. Awareness of the potential of the FIU's database as an additional resource in the course of ML and predicate offence investigations has improved gradually over the years. However, its full potential may still be underutilised.

4. The number of STRs has increased considerably in the period under review, especially as far as banks are concerned. However, the quality of a large portion of STRs is still not up to a satisfactory level, according to the FIU and underreporting within certain sectors continues to pose a problem. There are some concerns regarding the non-reporting of FT STRs by the MVTS sector. These shortcomings have a negative impact on the entire AML/CFT chain as they reduce law enforcement opportunities to identify and investigate ML, associated predicate offences, and FT.

5. None of the declarations submitted by the Customs Department to the FIU has ever resulted in the initiation of an analysis. The Customs Department does not often detect false or non-declarations and suspicions of either ML or FT have never been identified at the borders as evident from the figures in the table.

6. The FIU has a reasonably thorough analysis procedure. The analysts met on-site were knowledgeable and have the ability of producing complex analysis. There are factors which may limit the effectiveness of the analysis process, particularly the lack of advanced IT tools for STR analysis, limited human resources and absence of a prioritisation mechanism for STRs.

7. LEAs, especially the FCIS, have to some extent used FIU analytical products to pursue ML and associated predicate offences effectively. However, a large portion of FIU products concern tax matters and are referred to the STI, which is not a law enforcement authority. LEAs do not initiate a pre-trial investigation for ML where FIU dissemination products do not contain a clear link between the predicate offence and the ML. There is also a residual concern that the FIU is not yet fully operational independent and autonomous despite the recent legislative amendments to its statute.

8. The FIU has effective cooperation mechanisms with all competent authorities and uses these channels effectively. There are no concerns about the confidential handling of information.

Immediate Outcome 7

1. At the beginning of the period under review, opportunities to identify ML in the course of predicate offence investigations were not explored to the greatest extent possible, the degree to which ML was targeted by each LEA varied and the approach to proactively pursue ML cases was fragmented.

2. Latterly, concrete efforts have been made to target ML as an offence worth pursuing in its own right, separately from the prevention and repression of predicate criminality, as a result of greater enforcement of prosecutorial policies, which classify ML as a high priority offence. This is supported by a number of on-going investigations presented to the assessment team, some of which have already resulted in ML convictions. However, a national ML-specific operational policy is needed to ensure a more uniform and effective approach across all LEAs involved.

3. The majority of cases appear to be identified in the course of an investigation of a predicate offence or on the basis of information from domestic or foreign competent authorities. Few ML cases were identified on the basis of a referral from the FIU. Financial investigations (both at the intelligence and pre-trial stage) are not yet extensively used to identify ML, although there has been significant progress in recent years.

4. The number of investigations for ML appears to be low when compared to the number of criminal offences reported in the period under review and the number of investigations has been on the decline. However, there has been notable improvement in the quality of investigations and the

ability to investigate complex ML cases has developed significantly closer to the date of the on-site visit.

5. There are some very encouraging signs indicating that LEAs and judicial authorities have started pursuing ML related to the predicate offences which pose the highest threats, particularly ML related to corruption and organised criminality. However, these results were achieved very close to the date of the on-site assessment. Overall, in the period under review, ML related to the predicate offences which pose the highest threats (organised crime, fraud and corruption) did not receive sufficient attention. There have not been many ML cases yet involving misuse of corporate structures and fictitious companies, which appear to be used in trade-based ML.

6. In 2017 and 2018, some major ML convictions were achieved, involving substantial sums and complex laundering schemes. However, most ML convictions are for self-laundering. While a conviction for a predicate offence is not necessary to achieve a ML conviction, there is some uncertainty as to the level of evidence that would be needed to convince the judiciary that funds derive from criminal activity. The use of circumstantial evidence to prove that the launderer knew that the property derived from criminal activity is not always accepted by the courts, although there are clear precedents. It is therefore not surprising that the number of third party and stand-alone ML convictions is limited.

7. A review of the convictions provided to the assessment team indicates that the judiciary applies a strict interpretation of the material elements of the ML offence under Article 216. For instance, in some cases, the court did not consider the transfer of funds through a bank account to constitute conversion or transfer of property for the purposes of Article 216 and acquitted the accused of the ML charges. It should be noted, however, that on a number of occasions the decisions of the courts have been appealed, which demonstrates a proactive approach by the Prosecution Service.

8. The sanctions under Article 216 have the potential to be dissuasive. However, sanctions have not been used effectively and dissuasively. Many of the sentences involved a fine, often lower than the laundered proceeds. Most imprisonment sentences were suspended. There have not been many ML convictions for legal persons, despite the fact that legal persons feature recurrently in cases presented by the authorities.

Immediate Outcome 8

1. Depriving criminals of proceeds of crime is a policy issue endorsed at the highest levels within the prosecutorial and law enforcement structures in Lithuania. The PG issued recommendations to conduct financial investigations, which are binding on all LEAs. Financial investigations are conducted regularly in parallel with the investigation of proceeds-generating crimes in order to trace, identify and seize proceeds of crime from the very start of the investigation to ensure eventual confiscation.

2. At the beginning of the period under review, the emphasis of financial investigations was on developing the financial profile of the suspect, rather than tracing the proceeds of crime and/or identifying the extent of criminal networks.

3. The complexity and sophistication of financial investigations appears to have improved in the last couple of years. It has now become increasingly common, when investigating complex proceeds-generating crimes, to set up joint investigation teams, involving case investigators, intelligence

officers and financial specialists. However, further progress is needed to continue enhancing the quality of financial investigations, especially within the SIS.

4. Data on the volume of assets seized and confiscated in relation to ML and other predicate offences and on restitution to victims demonstrates a visible improvement in the implementation of seizure and confiscation requirements, especially when compared to the situation at the time of the 4th Round MER adopted in 2012. While the volume of seized assets has increased significantly, the volume of confiscated assets remains somewhat modest.

5. There is universal understanding that property as defined in the CC covers all types of property listed in the FATF Methodology, including virtual currencies. All types of property have been confiscated. However, the practice in pursuing laundered property, indirect proceeds and co-mingled property is not developed.

6. The absence of a sound mechanism at the border to identify suspicious transportation of cash at the borders and confiscate such cash raises significant concern.

7. While there are mechanisms in place for the management of seized and confiscated assets, they may no longer be sufficient in the event of an increase in seizure orders. There are no detailed procedures for the execution of confiscation orders which may have an impact on the effectiveness of the process.

Recommended Actions

Immediate Outcome 6

1. The use of financial intelligence developed through financial investigations at the intelligence stage should be widened to, inter alia, target ML and FT elements (in addition to unlawful enrichment and tax-related offences[31]), follow the trail of potential proceeds of crime and identify other involved parties, such as beneficiaries of transactions, to establish new or additional links and leads for investigations.

2. The authorities should take measures to improve the quality of STRs, including by: 1) determining whether the suspicious indicators need to be further enhanced; 2) holding discussions with banks to ensure that reporting is further aligned with the risks facing Lithuania; 3) assess whether the quality and reporting level by each bank are adequate; 4) hold awareness-raising activities with reporting entities facing a higher risk of ML/FT on reporting; 5) provide more systematic feedback to reporting entities on reporting; 6) consider why other reporting entities have not submitted any STRs (other than banks and MVTs); 7) consider whether the limited number of FT STRs is entirely in line with the risks that Lithuania faces.

3. The Customs Department should develop sound mechanisms to be able to detect false or non-declarations and suspicions of either ML or FT (which could arise even where declarations are submitted).

4. The FIU should re-calibrate its analysis and dissemination priorities to focus on the highest ML risks and make more effective use of its limited resources.

5. Enhance the technical capacities (IT tools) of the analysis function of the FIU and ensure that it is adequately resourced in terms of staff. Compliance responsibility should not deprive resources

[31] The authorities indicated that following the on-site visit measures were taken to update the PG's Recommendations accordingly.

from the analysis section. Compliance matters should be dealt completely separately from the analysis section.

6. LEAs should not refrain from initiating a pre-trial investigation for ML where FIU dissemination products do not contain a clear link between the predicate offence and the ML.

7. Strategic analysis should be conducted more systematically by the FIU. The strategic analysis products of the FIU should receive the proper level of attention and consideration by the GPO and LEAs and taken into account, where appropriate, when determining national LEA strategies.

8. The status of the FIU as an operationally independent and autonomous unit should be clearly established to elevate the status of the FIU and enable it to take an even more active and authoritative co-ordinating role in pursuing ML, particularly within the law enforcement sphere.

9. LEAs should be more proactive in requesting information from the FIU both at the intelligence and the pre-trial stage. Lithuania should also consider how the FIU's analysis potential could be used by all LEAs during intelligence gathering and investigations of ML, FT and related predicate offences and the identification and tracing of proceeds.

10. LEAs and the FIU should establish a feedback mechanism on the quality of disseminated products and their outcome, including the number of investigations, prosecutions and convictions resulting therefrom. Information provided should be broken down by ML, FT and predicate offences. The FIU should hold systematic meetings with all LEAs to discuss the use of FIU analysis products.

11. The FIU should improve the analysis of cash declarations with the aim of developing ML/FT cases in relation to cash crossing the border.

12. Re-consider the criteria in the analysis rules to ensure that STRs which could potentially lead to an investigation are not archived at the first and second stage of the analysis process and implement a risk-based prioritisation system for the treatment of incoming STRs to focus the analysis on the most risky and urgent suspicious transactions or activities.

Immediate Outcome 7

1. Lithuania should strengthen existing law enforcement strategies by developing a ML-specific operational policy which should:

a) clearly set out how each LEA is to identify and initiate ML cases, including through parallel financial investigations both at criminal intelligence and pre-trial stage, on the basis of FIU disseminations, in the course of the investigation of a predicate offence; and through the sharing of information between LEAs; and

b) include measures to (1) pro-actively identify ML elements at the earliest stages of suspicion and consequently initiate ML investigation rather than focussing only on unlawful enrichment; and (2) trace the sources and destination of proceeds of crime.

2. Law enforcement efforts should be in line with the ML risks. In particular, LEAs should continue targeting more complex and sophisticated types of ML with special attention to cases which involve the misuse of fictitious companies, trade-based ML, fraud, organised crime, corruption and ML related to foreign predicate offences). In complex criminal schemes, LEAs should extend their investigation with the aim of identifying the person(s) who ultimately controls and benefits from the scheme.

3. The PG Recommendations should be updated to improve the ability of LEAs and the Prosecution Service developing 'objective circumstantial and indirect evidence' when proving: (1) that the property is the proceeds of crime, in the absence of a conviction for the underlying crime; and (2) intent and knowledge of the launderer.

4. LEAs and the PGO should continue challenging the judiciary with stand-alone ML cases where it is not possible to establish precisely the underlying offence(s) but where the courts could infer the existence of predicate criminality from adduced facts and circumstances. Lithuania should consider introducing provisions in the CC which further clarify that when proving that property is the proceeds of crime, it should not be necessary that a person be convicted of a predicate offence. More cases related to professional third party ML should also be brought forward.

5. Training should be provided to the judiciary on the interpretation of the mental and material elements of the offence in line with the Vienna and Palermo Convention and internationally-accepted practice.

6. Analyse and review current sentencing practices for ML, and engage in dialogue with the judiciary on the results, with a view to developing a greater understanding of the need for a ML sanctioning regime which is both appropriate and dissuasive.

7. LEAs, the Prosecution Service and the judiciary should apply the existing legal framework governing criminal liability for legal persons in the area of ML more actively.

Immediate Outcome 8

1. Revise the PG's Recommendations on financial investigations to extend their scope beyond the financial profile of the suspect and include reference to the identification and tracing of movements of the proceeds of crime and identifying the extent of criminal networks and/or the scale of criminality.

2. Strengthen the enforcement of the PG's Recommendations to ensure that all types of property (laundered property, co-mingled, property of equivalent value and instrumentalities) are provisionally restrained and confiscated upon conviction.

3. The implementation of financial investigations by the SIS should be improved.

4. Additional human and technical resources and training should be provided to the Customs Department (including the Customs Criminal Service) to strengthen the mechanisms for the identification of non-declared cash and false declarations. In addition, urgent legislative measures should be taken to introduce the powers referred to under criteria 32.4 and 32.8 and introduce a requirement to declare cash transferred through mail and cargo.

5. The Prosecution Service and all LEAs should develop further the use of intelligence to identify suspicions of ML/FT or predicate offences relating to the transportation of cash at the (intra- and extra-EU) borders.

6. Lithuania should establish centralised mechanisms for the identification, tracing and management of seized and confiscated property, which could serve the functions of an asset recovery and management office.

7. Practical guidance should be developed to govern the activities of bailiffs in terms of execution of enforcement orders.

8. Statistics should be maintained on the enforcement of confiscation orders by bailiffs and the STI in criminal procedures.

Immediate Outcome 6 (Financial intelligence ML/TF)

Use of financial intelligence and other information

Law enforcement-generated intelligence

104. The law enforcement community in Lithuania has a sound framework for the gathering of intelligence, which is underpinned by the Law on Criminal Intelligence (LCI). The LCI is used extensively to prevent and repress some of the crimes which pose a high ML threat in Lithuania, such as organised crime, fraud, drug trafficking, smuggling, tax evasion and corruption and to identify, trace and seize the proceeds generated by such crimes. Criminal intelligence investigations may be initiated where information suggests that certain crimes[32] are being planned, are being committed or have been committed. Criminal intelligence is gathered through the use of agents, interviews, inspections, controlled verification and delivery, imitation of a criminal act, stakeouts, surveillance, covert operations, etc.

105. One of the objectives of a criminal intelligence investigation under the LCI is the search for assets related to the commission of a criminal offence. This objective is fleshed out in the PG's Recommendations on Financial Investigations, which oblige LEAs to gather financial information and produce financial intelligence in parallel with a criminal intelligence investigation in relation to crimes which have generated material gain. Statistics, although not complete, demonstrate that financial intelligence is produced regularly in the course of a criminal intelligence investigation, particularly by a specialised unit of the FCIS. Financial intelligence is generated through requests for information, pursuant to the LCI, to any person, public or private (such as registries of legal persons, property, vehicles, banks and other FIs, etc.) by specialised units conducting financial analysis within the FCIS and the Police. The authorities presented a number of cases demonstrating their ability to identify and trace proceeds of crime through the use of financial intelligence generated through the application of the PG's Recommendations. Two such cases are presented below.

Box 6.1: Financial intelligence generated by LEAs

Organised Crime Case

The Organised Crime Investigation Board of Vilnius County Police Headquarters conducted a criminal intelligence investigation in connection with an individual (V.R) who organised and distributed narcotic and psychotropic substances. According to the data available, the drugs were intended for the Lithuanian market. At the criminal intelligence stage, attention was paid not only to gathering evidence on the primary drug-related crime but also to the estimation and tracing of the material gain, through the use of financial intelligence, derived from crime. Requests for information were sent to banks, public registries, etc. and the information was analysed. Following this process, the assets owned by V.R. were established (that is, a plot of land with objects belonging to it, 3 vehicles, cash, antiques and other items), amounting to more than EUR 118,000, which, it was suspected, were transferred to family members and close relatives, upon concluding fictitious transactions. After a long-term investigation, in October 2016 a pre-trial investigation was commenced. Two individuals, linked to organised crime structures active in Vilnius county, were

[32] Grave crimes, serious crimes (including ML and FT) and certain less serious crimes (Article8, LCI)

detained in relation to disposal and distribution of narcotic and psychotropic substances in large quantities. At the prosecutor's and court's decision, the abovementioned assets were seized, both at the pre-trial investigation stage and upon case referral to court. During the judicial proceedings a request to confiscate the assets will be made since there are grounds to believe that the assets are derived from crime.

Tax-related Case

On 28 March 2018, a criminal intelligence investigation was launched following the receipt of information that certain Lithuanian nationals sought to evade taxes in relation to trade in vehicles registered in Lithuania. During the criminal intelligence stage, through the use of financial intelligence, it was determined that the persons involved had only declared EUR 4,000 as income generated in 2015-2018; all the individuals were unemployed and were not in possession of movable or immovable property, although the investigation revealed that in 2015-2018 this group of individuals executed the total of purchase-sale contracts for the sum of EUR 1,746,412. While conducting the financial investigation, the following assets were identified: 24 vehicles, cottages, a garage, 2 flats amounting to the total of EUR 450,000. Upon collection of sufficient data suggesting that the individuals committed criminal offences laid down in Articles 202 (Unauthorised Engagement in Economic, Commercial, Financial or Professional Activities) and 189-1 (unlawful enrichment) of the Lithuanian Criminal Code, in May 2018 a pre-trial investigation was initiated. During the pre-trial investigation, the financial intelligence generated as part of the criminal intelligence investigation allowed the LEA to qualify the criminal act not only in accordance with Article 202 of the Criminal Code but also in accordance with Article 189-1. Additionally, the property traced and identified during the investigation constituted the objects of pre-trial investigation which, subject to the prosecutor's decision, were seized, for eventual confiscation.

106. While the cases above demonstrate a positive use of financial intelligence at the criminal intelligence stage, it is not clear that the scope is yet wide enough. For instance, it appears that criminal intelligence officers do not analyse the financial transactions of the suspect and connected persons to follow the trail of potential proceeds of crime and identify other persons, such as beneficiaries of transactions, to establish new or additional links and leads for investigations. This is likely due to the fact that the part of the PG Recommendations[33] which deals with financial investigations at the criminal intelligence stage is very much focussed on determining whether a person has failed to declare income to the STI and whether the suspect is in a position to prove that the income sources were lawful, and as a result whether elements of the offence of unlawful enrichment (Art 189[1] CC) may be established. It is therefore doubtful whether financial intelligence at the intelligence stage is being used to develop evidence related to ML and FT.

FIU-generated intelligence

107. The FIU has direct/indirect access to and uses a very broader range of financial, law enforcement and administrative information, which also includes information from STRs, threshold reports, cross-border declarations and commercial databases[34]. The vast majority of registers are

[33] The PG's Recommendations are expected to be revised in 2019.

[34] Centre of registers: Real Property Register and Cadastre, Register of Legal Entities, Population Register, Mortgage Register, Information System of the Legal Entities participants, Judicial Officers Information System; Ministry of the Interior of the Republic of Lithuania: Register of suspect, accused and convicted persons, Population register: the particulars of the person, State enterprise Registry, Register of Legal Entities, Customs of the Republic of Lithuania: declarations, Border crossing database, The Schengen Information System (SIS),

accessed directly. The FIU can also request additional information (including documents or data covered by financial secrecy) from any public authority or reporting entity, regardless of whether such entity had previously submitted an STR. Information requests are a daily occurrence and information is generally obtained in a timely manner. Although statistics are not maintained, no challenges were identified by the assessment team in this respect. In the course of its analysis, the FIU accesses financial information (mainly in the form of bank statements) in order to analyse financial flows. Law enforcement information which would typically be obtained includes criminal records and on-going investigations. Since the FIU in Lithuania is a law enforcement-type FIU, it has access to all law enforcement databases within the country except for the database of the SSD. Administrative information, such as information from the company registry (on shareholders, directors, beneficial owners, etc.) and the land registry are used to develop a financial profile of the suspect and identify links with third parties.

108. Awareness of the FIU as a source of financial intelligence both during the pre-trial and intelligence stage is improving gradually, as evident from the number of requests made by LEAs shown in the table below. The figures are, however, still quite low, although they have been increasing in recent years for the Police and SSD. Due to the close cooperation that the FIU maintains with other LEAs, which is often based on personal contact, the FIU is prompt in responding to LEA requests. Requests made by LEAs typically involve information concerning STRs, account holders and information from foreign FIUs. For instance, during an intelligence or pre-trial investigation, the Police may request the FIU to confirm whether the person under investigation is known to the FIU as a result of an STR. The FIU is also generally requested to identify bank accounts held by foreign entities or individuals in relation to requests received by the Police via the ARO. Further information on the use of FIU-generated intelligence by LEAs is provided under core issue 6.3.

109. The number of requests made by the SSD to the FIU in relation to FT cases has increased significantly over the period under review. The assessment team was informed that the SSD requested information from the FIU on the financial activities of individuals and entities and sought to assess their possible involvement in illegal activities, including FT, and to assess a potential threat to national security. The SSD determined that no further actions regarding the CFT were required. No further explanations were provided.

Table 7: Information request from LEAs to the FIU

European Criminal Records Information System (ECRIS), Visa Information System, Administrative Offences register; State enterprise Registry: Vehicles register; State Tax Inspectorate Under the Ministry of Finance of the Republic of Lithuania (declarations; information of accounts); Customs of the Republic of Lithuania: Declarations; transit declarations etc., Recognition System of the vehicle registration number (NAS); Social Insurance registry (SODRA); Lithuanian Court information system (LITEKO); State border guard service at the Ministry of the Interior of the Republic of Lithuania: Border crossing database; Police Department under the Ministry of the Interior of the Republic Lithuania: Information System of the accidents, Public Procurement Office: Central public procurement Information System; National Paying Agency under the Ministry of Agriculture of the Republic of Lithuania: NPA portal.

Year	Number of incoming requests for assistance by LEAs	Police Department	Prosecutors	SIS	Customs	State Border Guards	STI (not LEA)	other agencies	SSD
2013	77	49	-	6	5	1	6	1	9
2014	80	28	1	7	4	2	9	9	20
2015	108	24	3	9	1	1	2	7	61
2016	177	64	2	7	3	1	4	2	94
2017	185	69	1	4	4	-	4	1	102

STRs received and requested by competent authorities

110. The FIU is the central authority for the receipt of reports submitted by REs, which comprise both STRs and CTRs. STRs are based on the REs' internal controls and a list of criteria on suspicious monetary operations or transactions approved by the FIU. CTRs are reported when transactions or monetary operations in cash amount to or exceed EUR 15,000. STRs and CTRs are submitted securely in electronic format through a dedicated webpage on the FIU's website. The FIU also receives cash declarations made at the border.

Suspicious Transaction Reports

111. The total number of STRs has followed a constant upward trajectory in the period 2013-2017, with a slight dip in 2014. In 2017, the FIU received 835 STRs, more than twice the number of STRs received in 2013, which was 400. As show in table below, most STRs were submitted by the banking sector, which is by far the most material sector in Lithuania, followed by MVTS, the second most material sector, and casinos. Reporting by other FIs and DNFBPs is very low, in some cases non-existent. Both the FIU and the BoL are satisfied with the increase in number of STRs, especially by banks, which, in their view, is likely the result of regular feedback provided to REs and intense awareness-raising campaigns conducted over the years. As noted under IO4, banks have, in recent years, improved their internal control systems, including the implementation of advanced IT tools.

112. The assessment team is, however, of the view that the number of STRs submitted by the MVTS sector is low, given the volume of funds that the sector processes annually and the risks associated with cash, which is often transferred in and out of the country through this sector, which may also involve higher risk countries. One major MVTS provider operating in Lithuania licenced in another EU member state only submits STRs to the FIU voluntarily as it is not legally bound to do so in Lithuania. It also transpired that transactions to certain high FT risk countries were not reported to the FIU. The fact that real estate agents have never filed any STRs and the low numbers of STRs from notaries raise concern, considering that real estate is known to have been used to launder funds on behalf of organised criminal groups. It is quite positive that casinos report regularly, since the risks emanating from this sector are not insignificant[35]. Although TCSPs are reporting entities under the AML/CFT Law, they have not yet been subject to a registration requirement and remain unsupervised. It is therefore not surprising that no STRs have originated from this sector. This raises

[35] The authorities indicate that of the total number of STRs reported by casinos, 3 reports were disseminated to LEAs and 1 to the SSD.

significant concern in view of the risks posed by fictitious companies, where TCSPs might be acting as nominee directors or shareholders. The authorities have not considered whether the reporting levels by the other REs e.g. currency exchange, insurance, securities, etc. are adequate. For instance, in one of the cases referred to under IO 7, reference is made to the laundering of funds through the purchase of securities.

Table 8: ML-related STRs

Number of STRs					
	2013	**2014**	**2015**	**2016**	**2017**
Banks	204	179	226	302	509
Insurance sector	2	2	3	0	5
Securities sector	1	0	0	0	0
Investment firms	0	0	0	0	0
Currency exchange	0	0	0	0	2
Bailiffs	1	1	2	0	1
Casinos	46	47	89	56	66
Real estate agents	0	0	0	0	1
DPMS	1	1	0	0	0
Lawyers	0	2	0	0	2
Notaries	4	7	8	6	32
Accountants	0	2	0	0	2
Auditors	0	0	0	0	2
TCSPs	0	0	0	0	62
MVTS	117	52	81	68	71
Other professionals (including private citizens, the Post and credit unions)[36]	15	35	53	88	47
Fintech co's	0	0	0	0	0
TOTAL	391	328	462	520	802

113. Given the materiality of the banking sector, the assessment team deemed it necessary to analyse the reporting patterns of each individual bank more closely. The figures are presented in the table below, where banks are classified in accordance with their market share. Looking at the table, it is difficult to make any judgement on whether there has been a positive evolution across the entire banking sector in terms of reporting. While the number of STRs has increased within the sector collectively, the patterns at institutional level vary year on year, with some banks (particularly the two biggest banks) registering a progressive decrease. In addition, these decreases in reporting do not appear to be correlated with an increase in quality of the reporting. Although the assessment team is not in a position to reach a definite conclusion on whether the total number of STRs submitted by banks is sufficient, it is likely that the figures are still not at a satisfactory level. This conclusion is deduced from the fact that banks receive large volumes of requests from the FIU and LEAs, which might indicate that REs may sometimes fail to identify suspicious transactions or activities. It could also be argued that the total number STRs in 2017 (509) compared to the total number of banking sector customers (4,548,776) is relatively small.

Table 9: ML-related STRs filed by banks

[36] The authorities indicated that the category 'other professionals' refers to private citizens, the Post and credit unions. It is unclear why these institutions and private citizens are categorised under one heading. In the period under review, the Post did not submit any STRs, while credit unions filed 7 in total. The rest were filed by private citizens. It is also not clear what type of STRs are filed by private citizens.

Number of STRs					
	2013	**2014**	**2015**	**2016**	**2017**
Total	**204**	**179**	**226**	**302**	**509**
BANK 1	24	27	16	10	16
BANK 2	66	24	21	22	18
BANK 3	25	29	22	30	51
BANK 4	1	1	-	-	-
BANK 5	2	8	16	9	7
BANK 6	8	10	10	82	145
BANK 7	29	28	44	38	48
BANK 8	7	4	2	8	16
BANK 9	29	29	62	89	126
BANK 10	11	19	33	14	54
BANK 11	2	-	-	-	-

114. The FIU is of the view that, while the quality of STRs has been improving, much further progress is needed. A large proportion of STRs coming from banks continues to be either defensive in nature or else focussed on predicate offences (e.g. bank customer being defrauded). It was indicated on-site that in some banks the percentage of poor-quality STRs could go up to 80%. The vast majority of STRs are based on the list of criteria approved by the FIU. Some STRs are based on the existence of multiple criteria. The two most common reasons for submitting an STR are the carrying out of (1) transactions without any clear economic basis and (2) transactions that are not consistent with the customer's profile or transactional patterns. Other recurring reasons include the use of a bank account as a transit account and challenges in obtaining information (e.g. customer is never available, frequent changes in contact details, etc.). The rather generic nature of the criteria most frequently used to justify submitting an STR would appear to be one of the contributing factors underlying the high percentage of poor-quality STRs. The assessment team is of the view that overreliance on FIU-approved criteria is a very likely possibility.

115. The large majority of STRs are related to tax matters, which reflects the risks that Lithuania faces to some extent. However, without a targeted approach in place, this may influence the entire AML/CFT chain. Where it is known, STRs are related to other underlying offences: fraud (social engineering, VAT fraud), misappropriation of property, criminal acquisition of property, unauthorized engagement in economic or professional activity and forgery of documents. The FIU rarely receives STRs related to other types of crimes which constitute a significant ML threat such as corruption[37] and organised criminality involving various types of trafficking and smuggling. A substantial proportion of STRs relates to cash transactions, which is positive considering that cash is a threat in Lithuania. Most STRs relate to Lithuanian natural and legal persons (for instance, in 2017, STRs related to 654 Lithuanian natural persons, 247 Lithuanian legal persons, 330 foreign natural persons and 120 foreign legal persons). This appears to be in line with the risk-profile of Lithuania where business is not predominantly internationally-oriented.

116. It is not clear whether there have been any FT-related STRs. The FIU advised that it does not maintain a break down STR statistics in terms of ML and FT and that materials have been disseminated to the SSD (responsible for the investigation of FT) following the analysis of FT-related STRs. While the assessment team could not determine the exact figure of FT-related STRs, it is likely that there have not been many such instances. While banks are very much aware of the risks

[37] For instance only a few case reports were sent to SIS by the FIU.

associated with FT, in discussions with certain representatives of the MVTS sector onsite, the assessment team came across cases which, on the face of it, would have warranted the submission of an STR for suspicions of FT.

117. The authorities have not identified any cases of tipping off following the submission of STRs. The assessment team found no reason to believe that this has ever been an issue when interviewing private sector entities. All persons interviewed were found to be very much aware of the consequences of disclosing the fact that an STR had been submitted outside of the authorised reporting channels.

118. Overall, the assessment team is of the view that major improvements are needed to achieve an effective STR regime. The shortcomings related to the reporting of suspicious transactions have a negative impact on the entire AML/CFT chain, as they reduce law enforcement opportunities to identify and investigate ML, associated predicate offences, and FT cases.

Cash Transaction Reports

119. As one of the measures to manage and mitigate the risk arising from the high circulation of cash, Lithuania introduced a cash transaction reporting requirement i.e. transactions in cash amounting to or exceeding EUR 15,000 must be systematically reported to the FIU. The implementation of the regime has been rather successful within the most relevant sectors, notably the banking, casino, notarial and MVTS sectors. This has not been the case in the real estate sector, although the gap has been largely mitigated through reporting by notaries. The authorities have not identified many instances where this requirement has not been observed. The information gathered through these reports has been very useful to the FIU and other authorities as an additional information resource when developing intelligence in relation to STRs. All CTRs are filtered through an automated process to identify suspicions which deserve further attention. Many CTRs are forwarded to the analytical unit of the FIU for further analysis and ultimately result in disseminations for further investigations to LEAs. The CTR database also constitutes an additional valuable resource in the analysis of STRs. However, it is unclear whether any of the CTRs have actually resulted in any ML/FT investigations, prosecutions or convictions.

120. An IT system[38] was implemented in 2015 to facilitate the transmission, receipt and processing of large volumes of information obtained through CTRs. Upon receipt of a CTR, the system automatically assigns a risk scoring, based on 40 different risk criteria[39], which are updated from time to time taking into account the changing nature of risks. The system is directly connected to 14 internal and external databases and draws upon information contained therein to reach a more informed rating.

Table 10: CTRs registered in the Document Management and Data Processing System (DMDPS)

Number of CTRs					
	2013	**2014**	**2015**	**2016**	**2017**
Banks	563,982	630,049	585,417	546,139	562,620
Insurance sector	1	0	1	0	0

[38] Money Laundering Prevention Information System (MLPIS) of the Document Management and Data Processing System (DMDPS)

[39] E.g. person withdraws money in cash and crosses the border without making a declaration, person with low salary deposits large sum of cash in a bank account, person featuring in a STR purchases real estate, etc.

Securities sector	0	0	0	0	0
Investment firms	0	0	0	0	0
Currency exchange	0	0	0	0	0
Bailiffs	1	2	1	1	1
Casinos	36	52	121	49	53
Real estate agents	0	0	0	0	0
DPMS	0	0	0	0	0
Lawyers	0	0	0	0	0
Notaries	13,951	14,988	11,888	10,632	9,383
Accountants	0	0	0	2	8
Auditors	1	90	20	12	4
TCSPs	0	0	0	0	0
MVTS	1,693	1,312	1,305	1,744	892
Other professionals	370	336	238	246	874

Cross-border declarations

121. The Customs Department submits information on incoming and outgoing cross-border cash declarations to the FIU on a weekly basis. The Customs database is updated instantly when new cash declarations are filed. The figures are available in the table below. This information is treated by the FIU in the same manner as a CTR and is subject to the same automated procedure. However, the FIU confirmed that, to its knowledge, none of the declarations has ever resulted in the initiation of an analysis. The Customs Department very rarely detects false or non-declarations and suspicions of either ML or FT have never been identified at the borders as evident from the figures in the table. It was indicated that the Customs Department has limited resources, expertise and training to do so. Additionally, they do not have access to certain databases (such as the PNR[40]) and have not been provided with ML/FT indicators to assist them in exposing false/non-declarations and suspicions of ML/FT. Furthermore, their ability to restrain cash for a limited period of time is very restricted. It should also be noted that there is no requirement to declare cash transferred through mail and cargo. Overall, information from the Customs Department has not served as an effective resource to develop intelligence for ML and FT purposes. This is a significant shortcoming, in view of the high ML and FT risks associated with the inflow and outflow of cash through the borders.

Table 11: Incoming and outgoing cross-border cash declarations to the FIU

Year	Number of declarations		Non-declarations	False declarations
	Incoming	Outgoing		
2013	5,190	510	5	5
2014	3,898	344	10	0
2015	1,250	242	7	1
2016	816	258	5	1
2017	1,275	175	7	1

Operational needs supported by FIU analysis and dissemination

Operational analysis

122. The analysis of STRs comprises two levels, which essentially breaks down the process into a two-stage approach. The analysis starts at level two, where information accessible through the FIU

[40] Passenger name record

system (STRs, CTRs, direct access to databases) is gathered and analysed briefly. Within 10 days, the analyst working on the case makes a proposal to the head of the FIU on the next steps in the process i.e. whether (1) a level one (more in-depth) analysis should be initiated (based on the grounds described in the paragraph below); (2) the case should be archived (this would normally be the case where the FIU has gathered sufficient information that indicates that no unlawful activity has taken place or where there is insufficient data demonstrating that an unlawful activity has taken place) (3) disseminate information obtained through a level 2 analysis to the relevant domestic or foreign competent authorities, where there are sufficient grounds to conclude that unlawful activities have taken place. The evaluators are of the view that the threshold to archive STRs is too high (no statistics on the number of archived cases are available). The analysis conducted at level two is too limited to enable the FIU to gather sufficient information that indicates that no unlawful activity has taken place. Besides, as indicated in the paragraph below, it appears that the only cases that are taken to level one are those where there are clear indications that unlawful activities have taken place. It is not clear what would happen with cases which are unusual, complex and suspicions but in relation to which there is insufficient data on unlawful activity identifiable at the first stage of the analysis process. It is also the view of the assessment team that the 10-day period may be too long in urgent cases.

123. A level one analysis is initiated where the following circumstances are established during the level two analysis: a transaction has been suspended by the FIU following the receipt of the STR; there are clear indications that unlawful activities have taken place (this seems to overlap with (3) above which requires immediate dissemination where there are sufficient grounds indicating the existence of unlawful activity); the subject of the STR is a person designated under FT TFS (the authorities indicate that while there is a requirement for REs to freeze such funds, the FIU would still conduct an analysis to determine the type of activity that is conducted by these persons in Lithuania. The assessment team notes that the analysis manual does not refer to FT cases in general other than those which are TFS-related. It is not clear what procedure would be followed in these cases); there is relevant information within the FIU database on the persons reported in the STR; the person involved in the STR is subject to a past or an on-going criminal investigation; the STR involves amounts which are higher than EUR 200,000 (it is not clear how was this figure determined. It appears to the assessment team to be rather high. It is unclear whether an STR which involves lower sums lower would be archived).

124. During the level one analysis, further information is obtained by the analyst. This may include additional information from REs, information from domestic authorities, information from foreign FIUs, etc. At this stage, the analyst conducts a more in-depth analysis with the aid of various IT analytical tools. The assessment team found that the analysts met on-site displayed a deep understanding and knowledge of their functions. A number of sanitised cases which the assessment team inspected revealed that the analysts have the ability to conduct complex analysis.

125. There are some factors which may limit the FIU's ability to perform its analytical function at optimum capacity. The IT tools no longer appear to be adequate in light of the upward trend in the number of STRs, which does not show signs of abating. The number of analysts, who are also responsible for compliance matters, was at the lower end of the scale compared with the number of cases which were on-going at the time of the on-site visit. For instance, at the end of 2017, 8 analysts were analysing 883 STRs. Some of the analysts met on-site were dealing with upwards of 50 cases at one time. It was admitted that the analysts could in fact only deal with 2 or 3 cases simultaneously which meant that the analysis of all the other cases was relegated to a future point in time. All of this

has had the effect of delaying the analysis of cases, including urgent ones. It was also noted that the prioritisation of cases is left at the discretion of each analyst, with no formal instructions being provided.

Strategic analysis

126. Although the FIU does not have a strategic analysis unit and strategic analysis is not conducted in a systematic fashion, the FIU has conducted a number of strategic analysis exercises on such topics as fund movements in offshore company accounts, cash withdrawals in the NPO sector, the use of foreign credit cards for cash withdrawals in Lithuania, the purchase of real estate in cash, etc. These reports were disseminated for law enforcement action. The strategic analysis products of the FIU do not appear to have received the proper level of attention and consideration by the GPO and LEAs and taken into account, where appropriate, when determining national LEA strategies.

Dissemination

127. The FIU disseminates cases to domestic LEAs for further investigation where it identifies possible indications of criminal offences (including ML, associated predicate offences and FT[41]). It also disseminates cases to the STI, which is not a law enforcement authority, and foreign FIUs. The table below refers to the number of cases, in aggregate form, disseminated to domestic LEAs following the analysis of STRs and the number of pre-trial investigations and convictions resulting therefrom[42].

128. **Table 12:** FIU disseminations to LEAs

Number of FIU disseminations per year and resulting pre-trial investigations and convictions				
	Under analysis at year end	**FIU reports disseminated to LEAs for investigation**	**Pre-trial investigations (ML and associated predicate offences)**	**Convictions (ML and associated predicate offences)**
2013	401	92	35	13
2014	335	79	24	9
2015	475	98	26	7
2016	541	110	16	0
2017	833	119	40	1
Total	**2585**	**498**	**141**	**30**

129. Based on these figures, the FIU disseminated around 19% of the cases that it analysed to domestic LEAs during the period under review. As mentioned previously, the FIU appears to be slightly ill-equipped in terms of staffing and analytical tools to cope with the increasing number of STRs that are submitted for analysis. This could explain the relatively low percentage of disseminations. Concurrently, the quality of STRs (as explained under core issue 6.2) remains questionable, which in turn has an impact on the number of cases which would give rise to a referral to LEAs. Looking at the figures further along the chain, it appears that a reasonable number of pre-trial investigations are initiated based on FIU disseminations. A number of convictions have also been achieved. This indicates that, to some extent, the FIU's dissemination process has supported the operational needs of LEAs. However, since disseminations are not classified according to type of offence (i.e. ML, predicate offence or FT), the assessment team could not determine the percentage of disseminations that relate to ML and purely predicate offences.

[41] The FIU does not make a distinction between the three and does not keep separate statistics.
[42] No data on prosecutions was provided

130. Some information is contained within the annual reports of the FIU on the type and number of pre-trial investigations initiated by the FCIS. For instance, in 2016, the FCIS initiated 8 pre-trial investigations for various predicate offences (swindling, misappropriation of property, handling of stolen property, unlawful activities of a legal entity, provision of inaccurate data on income, profit or assets, fraudulent management and forgery) and 10 pre-trial investigations for ML. Some of the ML investigations were conducted in conjunction with the pre-trial investigations for the predicate offences. The situation was broadly similar in 2017. While the FCIS indicated that it is satisfied with the quality of the analytical reports prepared by the FIU, it was pointed out that pre-trial investigations for ML are only initiated where there is a clear link between the predicate offence and the ML. There are no similar figures for the police. In discussions with various representatives of the Police on-site it was said that few FIU reports trigger any action and most are maintained in the Police database for intelligence purposes.

131. A breakdown of the disseminations to each recipient (STI, the FCIS, the Police, Foreign FIUs and others[43]) is provided below.

Table 13: Number of disseminations per competent authority

Number of FIU disseminations							
	2013	**2014**	**2015**	**2016**	**2017**	**total**	**percentage**
STI	51	50	71	65	83	**320**	**33.65%**
FCIS	65	52	41	50	67	**275**	**28.92%**
Foreign FIUs	11	25	34	32	31	**133**	**13.99%**
Police	14	13	38	36	25	**126**	**13.25%**
Others[44]	13	14	19	24	27	**97**	**10.20%**
Total	**154**	**154**	**203**	**207**	**233**	**951**	**100%**

132. The largest percentage of disseminations (33.65%) goes to the STI, which is not a law enforcement authority and deals with tax matters purely on an administrative basis. This would suggest that far too many resources appear to be dedicated by the FIU to the handling of tax-related cases during the analysis process. On a positive note, the large majority of the reports disseminated by the FIU trigger action by the STI to recover unpaid taxes. The other major recipient of FIU disseminations is the FCIS, which is the body responsible for the investigation of economic/financial crime and ML. It appears that the dissemination process has assisted the FCIS in its activities, as it has initiated a number of pre-trial investigations on the basis of FIU reports. The police, which investigates some of the highest ML-threat crimes, receives the lowest amount of disseminations. The SIS, responsible for the investigation of another significant proceeds-generating crime (corruption), has received very few disseminations from the FIU. The FIU disseminates a sizeable portion of its cases to foreign FIUs. The FIU indicated that these involve activities of foreign persons, who are not present in Lithuania. On balance, it appears that the dissemination process of the FIU is being used to some extent to identify and investigate ML and associated predicate offences. It is not clear to the assessment team that systematic feedback is provided by LEAs to the FIU to improve the dissemination process.

[43] The FIU indicated that the category 'others' includes the SIS, Customs, Military Forces, Ministries, Prison Department, etc. No further information was provided as to the outcome of these disseminations.
[44] No further breakdown was provided.

133. Turning to FT, it appears that there have been instances where a reporting entity reported suspicions of FT or matches with persons or entities designated under FT UNSCRs. As a result of further analysis by the FIU, reports were disseminated to the SSD for further intelligence actions (although these disseminations do not appear to feature in the statistics provided). Also, following a review of the non-profit sector by the FIU (referred to under IO 10) some cases were disseminated to the SSD. However, the assessment team is not aware that any FT investigations were launched. The authorities indicated that in these cases the suspicions were not confirmed.

Operational Independence and Autonomy

134. At the time of the on-site visit[45], there were some residual concerns that, despite recent legislative changes, the FIU, which is placed within the broader structure of the FCIS, in some limited respects, did not function as an entirely autonomous unit. For instance, while the Head of the FIU autonomously took the decision to disseminate reports, it was the Head of the FCIS which signed these reports, when they were sent to other LEAs. The same procedure applied to requests for information by the FIU to other state authorities and agencies. It also appears that the FIU is not in a position to develop its own policy and strategy. While there is nothing at all to suggest that the FIU is subject to undue political or government interference, these issues, to some extent, call into question its operational autonomy. In the assessment team's view this has wider implications on the FIU's authority within the entire AML/CFT chain at a national level. Reinforcing the independence and autonomy of the FIU would elevate the status of the FIU and enable it to take an even more active and authoritative co-ordinating role in pursuing ML, particularly within the law enforcement sphere.

Cooperation and exchange of information/financial intelligence

135. There are no impediments, statutory or otherwise, which hinder the exchange of information. The assessment team was satisfied through discussions it had on-site that all competent authorities are willing to share information with the FIU and do so when so requested. Where information is needed formally (either from or by the FIU), a written request is submitted through electronic channels. Restricted information is exchanged through confidential channels. The FIU has broad access to other government databases. Access is provided through secured channels. Due to close contacts that the FIU maintains with LEAs, co-operation may also take place informally. This generally facilitates and expedites the process of information sharing. The FIU provides joint trainings (generally with the FCIS) and exchanges information on risks and trends identified to other competent authorities. The FIU, in accordance with data provision agreements, provides information on FT-related monetary operations and transactions to the SSD. The STI and the SIS receive data on CTRs from the FIU.

136. Turning to feedback on the disseminations of the FIU, the authorities seemed to indicate that this happens on a periodic basis. However, the FIU stated that it did not maintain statistics on further actions taken by LEAs on the basis of disseminations (e.g. number of pre-trial investigations), indicating that feedback does not happen systematically. The SSD does not provide feedback at all on the FIU's disseminations.

137. All the information related to STRs, financial information and any other information is stored in the FIU database. The information system is independent and has no connection to outside sources;

[45] This matter was addressed through legislative changes after the on-site visit.

access to it is protected. The FCIS, which hosts the FIU, has no access to the FIU database, except for one IT specialist of the FCIS. Representatives of the FIU pointed out that the specialist has no right to pass information to third parties and has signed tipping off agreement. The specialist administrates the IT database of the FIU, since the FIU does not have its own IT specialist. The FIU premises can only be accessed by FIU staff through a personal electronic card. All the information exchange between authorities is provided through special secure channels. To the authorities' knowledge there have been no cases of tipping off in Lithuania.

Conclusion

138. **Lithuania has achieved a moderate level of effectiveness for IO 6.**

Immediate Outcome 7 (ML investigation and prosecution)

139. All LEAs[46] in Lithuania are competent to conduct pre-trial investigations of ML. In practice, all ML cases are investigated by the FCIS and the Police. The FCIS is an autonomous law enforcement body under the Ministry of Interior responsible for the investigation of violations of law against the financial system and related crimes[47]. At the Police, ML investigations fall within the responsibility of specialised economic crime investigation units. Where ML investigations relate to organised criminality they are conducted by organised crime investigation units. Where ML is investigated together with a crime against property which has generated illegal proceeds, the investigation may be undertaken by the property crime investigation unit[48]. In recent years, the SIS has also started investigating ML. The SIS is an autonomous law enforcement body accountable to the President and the Parliament of the Republic of Lithuania and is responsible for the investigation of corruption offences and the development and implementation of prevention measures against corruption and related crimes, including ML.

140. ML pre-trial investigations are organised, conducted and supervised by the Department for Criminal Prosecution of the General Prosecutor's Office. The Department for Criminal Prosecution of the Prosecutor General's Office of the Republic of Lithuania and specialised divisions of regional prosecutor's offices specialise in the fields of unjust enrichment and ML. There are no special AML divisions functioning within the Prosecution Service. Chief Prosecutors of departments in the Prosecutor General's Office as well as Chief Prosecutors of regional prosecutor's offices pass orders which designate specialisation in ML and unjust enrichment to the prosecutors in the Prosecutor General's Office and prosecutors in the regional prosecutor's offices. These orders are binding on the respective prosecutors[49].

141. The various law enforcement officers and prosecutors met on-site were found to possess the required skills and knowledge to perform their functions adequately and appear to do so with

[46] The Police, the State Border Guard Service, the Special Investigation Service, Military Police, the Financial Crime Investigation Service, the Customs Department, the Fire and Rescue Department, the VIP Protection Department.
[47] FCIS Law
[48] 17/10/2014 Order of General Commissioner of Police of the Republic of Lithuania No. 5-V-890
[49] Prosecutors' specialisation in ML and unjust enrichment is provided for in the original wording of 30 October 2012 Order No. I-318 (7 March 2017 wording of Order No. I-68). This order has been amended by subsequent orders of the Prosecutor General dated 23 December 2014, 25 October 2015, 7 March 2017 and 4 December 2017.

integrity. This is also the case with respect to the judiciary. To a large extent, there are no substantive or procedural aspects that hinder the investigation and prosecution of ML. Another positive aspect of the system is the on-going discussion taking place within the Prosecution Service on the practical challenges faced by prosecutors and law enforcement officers in pursuing ML and possible solutions to resolve such difficulties.

ML identification and investigation

Identification of ML cases

142. In recent years (especially in 2017-2018), efforts to identify and investigate ML in Lithuania have intensified as a result of various prosecutorial and law enforcement strategies that have been developed, which classify ML as a high-priority offence within the country[50]. Prior to that, in the first part of the period under review (2013-2016), ML did not appear to be prioritised by LEAs as an offence worth pursuing in its own right focussing instead on the prevention and repression of predicate criminality and the seizure of related proceeds. Consequently, opportunities to identify ML cases in the course of an investigation of a predicate crime were not explored to the greatest extent possible. The degree to which ML was targeted by each LEA varied and the approach to proactively pursue ML cases was relatively fragmented. The authorities agree that, while measures have already been set in train to improve the effectiveness of the system[51], further progress is required to target ML more systematically and in a holistic fashion, particularly due to the fact that various LEAs are involved in pursuing ML.

143. The authorities maintain that ML cases are identified either through a criminal intelligence investigation, in the course of an investigation of a predicate offence (e.g. initiated on the basis of a complaint by a victim or informant), following the dissemination of a report by the FIU, or upon receipt of information from a domestic or a foreign authority. Extrapolating from a review of cases which led to a ML conviction, in the absence of detailed statistics, the assessment team came to the conclusion that the majority of cases appear to be initiated by LEAs in the course of an investigation of a predicate offence or on the basis of information from domestic or foreign competent authorities. This was eventually confirmed also on the basis of various cases presented after the on-site visit (see Boxes 7.1 – 7.7). ML cases identified on the basis of a referral from the FIU were mostly taken forward by the FCIS. At the Police, these referrals have been developed to pursue predicate offences but less so for ML. Some LEAs put forward the view that unless there is a clear link between the laundering and a predicate offence in a referral by the FIU, a ML case is not taken forward.

144. The assessment team also considered whether proactive and parallel financial investigations have been used to identify ML. As noted under IO 6, financial investigations at the criminal intelligence were largely focussed on determining whether a person has failed to declare income to the STI and whether there is sufficient proof that the income sources of a person are lawful, and, as a result, whether elements of the offence of unlawful enrichment (Art 189[1] CC) may be established, without exploring further the material and mental elements of the ML crime. As noted under IO 8, the emphasis of financial investigations during the pre-trial investigation stage was, in most cases, on

[50] For instance, the Strategic action plan of the Prosecutor General's Office regarding crimes against financial system; National Risk Assessment Action Plan for the period 2016-2018 (Financial Crime Investigation Service)
[51] Following the on-site visit, new recommendations were issued by the Prosecutor General on 27 June 2018 (which will become effective on 1 January 2019) regarding financial investigations and focus on investigation of different methods of legalization of criminal proceeds.

developing a financial profile of the suspect. For instance, in discussions with certain LEAs, it appeared that when investigating complex criminal schemes (whether involving fraud, corruption, tax or organised criminality), the investigation focused on the front persons and did not go beyond those who were behind or organising those schemes. The overall result is that financial investigations, while being regularly conducted, did not frequently result in the identification and investigation of ML cases, especially at the beginning of the period under review.

145. The situation appears to have improved closer to the date of the on-site visit. The skills required to go beyond the front persons to identify the person ultimately controlling the criminal scheme have been developing over the last couple of years. The LEAs which investigate ML (i.e. the FCIS, the Police and the SIS) now have specialised officers responsible for conducting financial analysis. Furthermore, in the course of a pre-trial investigation, specialists or experts are being appointed[52] with increasing frequency. The authorities stressed that it has become more and more common to set up joint investigation teams, which also comprise financial analysts, criminal intelligence officers and forensic experts. Some case examples were provided after the on-site visit indicating that financial investigations carried out alongside the investigation of predicate offences (particularly fraud, tax evasion and drug trafficking) were used to uncover not only complex criminal schemes but also related ML involving, for instance, fictitious transactions and the use of offshore companies. One such case is presented in Box 7.1 below.

Box 7.1: *"Social engineering" Case*

Predicate crime: Members of an international organised criminal group, also involving Lithuanian citizens, defrauded various companies situated in different countries by posing as directors of the parent company in the United States of America (social engineering) and used Lithuanian companies to launder the proceeds.

ML (relevance to IO 7): Upon conducting a financial investigation alongside the investigation of the social engineering fraud, the investigators uncovered a total of 10 fictitious companies that had been established in Lithuania by front persons (mainly foreigners). It was established that the companies had opened more than 15 bank accounts with Lithuanian banks, which were used to launder EUR 3.5 million generated by the scam. The victims transferred money into the bank accounts of the fictitious companies, which were then transferred, through various layering operations, to foreign bank accounts, some of which were situated in offshore jurisdictions. The financial investigation revealed that money from the Lithuanian companies was transferred to over 300 foreign bank accounts. The investigation also revealed that the entire operation was run from Israel with members of the criminal group also based in Lithuania, Russia, France, Ukraine, and China. The proceeds were ultimately repatriated to Israel and the Russian Federation.

Identification of the case (relevance to IO 6): The FIU disseminated information to the Police following the analysis of a STR by a bank in relation to two monetary operations carried out through the bank account of one of the Lithuanian fictitious companies. The company had received two transactions from a company registered in Spain, which later transferred the funds through various operations to different bank accounts outside of Lithuania.

Seizure and freezing of property (relevance to IO 8): Part of the proceeds, i.e. EUR 1.5 million, were traced and frozen through formal and informal co-operation with foreign law enforcement authorities and prosecution services. In order to ensure a civil claim of EUR 2 million, property belonging to OCG members amounting to EUR 0.5 million, was also traced and frozen.

Formal and informal international co-operation (relevance to IO 2): information was exchanged through: (1) liaison officers of the FCIS who supplied information directly to foreign law enforcement authorities; and

[52] According to the PG's Recommendations on the Assignment of Tasks to Specialists and Experts

(2) a representative of the Prosecutor General's Office at EUROJUST. A JIT was established through EUROPOL (APATE group, set up specifically for the purposes of combating social engineering cases at the European level). Over 20 mutual legal assistance requests were sent to various countries worldwide.
Status of the case: Criminal proceedings will be instituted in the near future, which will also include ML charges.

Investigation of ML cases

146. In the period under review, a total of 267 ML investigations were conducted, as shown in the table below. In the same period, the number of reported criminal offences having the potential of generating proceeds was 175,000. While it is not expected that every single reported criminal offence will result in an investigation and not every investigation of a predicate crime will necessitate a ML investigation, the discrepancy between the two figures is considerable and supports the conclusion that LEAs have not been as proactive in pursuing ML, particularly, as already noted, at the start of the assessment period.

Table 13: ML investigations

	2013	2014	2015	2016	2017	Total
FCIS	20	24	20	10	12	86
Police	36	36	78	22	9	145
SIS	0	2	0	2	0	4
Total	56	60	98	32	21	**267**

147. The assessment team, however, acknowledges that, while the number of investigations has decreased, there has been a marked improvement in the quality of cases pursued in the period 2017-2018. This conclusion is based on the ML convictions achieved and case examples of ML investigations, which were under way during the on-site visit. The assessment team also recognises that there are various elements within the system that significantly add to the quality of investigations. For instance, the legal framework provides a solid basis for an effective criminal procedure. LEAs and the prosecution service appear to use all techniques and coercive measures to obtain evidence admissible in court (as evidenced by the cases in the boxes). The guidance and recommendations by the PGO have been very helpful in practice and their influence on the overall effectiveness is recognised and confirmed by the judiciary. It is also worth highlighting the ability of the system to effectively incorporate the performance and results of the criminal intelligence activity into criminal proceedings. There is no evidence that the length of criminal proceedings decreases the effectiveness of the system[53]. No ML cases failed due to statutory limitations.

148. The Prosecution Service pointed out that a more strategic view is being taken in relation to ML, choosing to focus resources on more complex ML cases. This position is supported by the following case examples.

Box 7.2: *Gasoil Case*

Predicate offence: this was a very complex case related to a criminal group involved in various criminal offences including forgery of documents, misappropriation of company funds, tax fraud, misuse of a company

[53] The average duration of pre-trial investigations completed in 2017 – 4 months. The part of pre-trial investigations lasting for over 9 months at the end of 2017 was 14.3%. (in 2015 was18,5%, in 2016 was 21,8%).

for unlawful activities, fraudulent management of accounts, abuse of power, bribery and embezzlement of property. For example, in one instance, through the use of fictitious agreements, funds were transferred between different companies controlled by the group as payments for fictitious services, as a result of which taxes exceeding EUR 2 million were evaded over a 6-year period. In another instance, through abuse of office by persons connected to the criminal group, a company involved in the gasoil business, suffered losses in excess of EUR 20 million. The scheme involved the payment of bribes exceeding EUR 3 million and USD 175,000.

ML element: Funds were laundered through complex schemes including withdrawal in cash, layering through financial transactions to different companies controlled by the criminal group, use of funds in legal economic activities and trading in securities, among other methods.

Identification of the case (relevance to IO 2 and IO 7): The case was identified by the FCIS following a criminal intelligence investigation upon receiving information from domestic authorities. During the criminal intelligence investigation actions of a covert nature were performed, witnesses were questioned, information was requested from foreign counterparts, financial investigations were conducted and searches, seizures and examinations of items were carried out.

Property seizure and freezing (relevance to IO 8): Assets were seized during the pre-trial investigation, including bank accounts, real estate, vehicles, motorcycles, etc. Upon conviction, the court ordered the confiscation of all assets from the crimes which in total amounted to EUR 11,367,190 and USD 175,549.

Status of the case: On 27 December 2017, the County Court of Klaipėda convicted three persons of ML, fraud, misappropriation, bribery, falsification of documents and fraudulent accounting. Sentences ranged from 2.9 to 7 years of imprisonment.

Box 7.3: *Bank Snoras Case*

In this case, money was laundered in various EU states, Switzerland, Panama, Russia, Ukraine and a number of offshore jurisdictions.

Predicate offence: The senior management of the bank misappropriated bank funds through 24 international transactions involving securities (at the nominal value of EUR 212,870,000) and 2 international wire transfer transactions (amounting to EUR 78,910,152.06) made to the personal bank accounts of the bank managers held in Switzerland.

ML element: The misappropriated funds were laundered through a series of complex loans (amounting to EUR 184,119,800.00) and various financial transactions to legal entities related to the suspects. The laundered funds were integrated into the financial system through the purchase of real estate, shares, cars and yachts, etc.

Identification of the case (relevance to IO 7): The case was initiated following information provided by the Bank of Lithuania on suspicions of misappropriation of funds. The ML elements were identified by the prosecutors and FCIS investigators, with the help of financial specialists, through a financial investigation. The financial investigation focussed on transactions carried out through banks accounts opened by 45 companies operating in Switzerland, Germany, Luxembourg, Austria, Latvia, Russia, Cyprus and Lithuania. Information was also obtained by means of testimony given by 50 witnesses, the analysis of various documents etc.

Property seizure and freezing (relevance to IO 8): On the basis of spontaneous exchange of information the prosecutors restrained assets amounting to a total value of EUR 161,947,946.00, including vehicles of the value of EUR 645,128.00, real estate of the value of EUR 27,458,695.00 (villas, houses, apartments in skiing resorts, apartments, homesteads, flats, cottages), money in bank accounts amounting to EUR 74,829,777.00 and other property rights amounting to EUR 59,014,346.00. The countries where these assets have been traced include Lithuania, Austria, Great Britain, Switzerland and France.

Formal and informal international cooperation (relevance to IO 2): 23 MLA requests regarding tracing

and seizure of assets were sent to 17 states; 17 MLA requests regarding collection of evidence were sent to 11 states (representatives from the Lithuanian Prosecution Service participated in the measures carried out in Switzerland, Austria, United Kingdom and Latvia). The Government of Lithuania assigned separate funds (EUR 145,000) to be used in the case for the purpose of business trips, translations, computer equipment, services of experts etc. Inquiries were sent via CARIN and FIU Egmont channel networks which resulted in 10 responses from different states.

Status of the case: The suspects were charged with misappropriation and ML and were in the process of being extradited from the United Kingdom to Lithuania on the basis of a European Arrest Warrant. However, they managed to flee to another country. An extradition request was sent to that country which was not executed. A process will be initiated to convict the two persons *in absentia* in 2019. The bank was in the meantime dissolved. At the initiative of Lithuanian prosecutors, a former employee of a Swiss bank was convicted as an accomplice.

Box 7.4: *Ūkio bankas Case*

Predicate offence: Assets were embezzled from the bank through three fictitious loans amounting to EUR 10,200,000, USD 10,000,000 USD and EUR 14,600,000 respectively to the majority shareholders of the bank through companies, two registered in Lithuania and one in the USA, which they controlled.

ML element: The proceeds embezzled through the first loan were laundered by means of 6 money transfers and acquisition of real estate in London, UK. In case of the second loan, the funds were laundered by means of 3 financial transactions involving money transfers and the fictitious payment of authorised capital in a company incorporated in the Republic of Belarus. In the case of the third loan, money was transferred to a company registered in Bosnia and Herzegovina. The money, in this case, was laundered by means of 440 financial transactions including money transfers, acquisition of shares, fulfilment of financial liabilities, funding of sports projects related to the shareholders (in Lithuania and abroad), funding of activities of related companies (in Lithuania and abroad), funding of real estate projects (in Lithuania and abroad) and use for personal needs of bank shareholders and their relatives.

Identification of the case (relevance to IO 2 and 7): Two of the fictitious loans were identified by the Bank of Lithuania and one by the FCIS in the course of its investigation into the other fictitious loans. The ML was identified by the FCIS through various financial investigations, which involved: in relation to the first fictitious loan, the analysis of bank account statements of 5 legal persons and information provided in response to 3 MLA requests sent to the UK and 2 to the Isle of Man; in relation to the second fictitious loan, the analysis of bank accounts statements of 4 legal persons and information provided in response to 1 MLA request sent to Belarus and 1 European Investigation Order to Italy; and in relation to the third fictitious loan, the analysis of over 850 bank account statements in relation to over 80 legal and natural persons and information provided by Bosnia and Herzegovina in relation to 2 MLAs and two meetings held with authorities from Bosnia and Herzegovina.

Seizure and freezing of property (relevance to IO 2 and IO 8): In total, assets amounting to EUR 44,720,266 and GBP 22,395,000 were restrained which also included real estate valued at EUR 3,224,268 in Lithuania and real estate valued at GBP 4,200,000 in the United Kingdom (flats, houses, cottages, homesteads, plots of land); EUR 41,005,394 in securities (shares of Lithuanian companies); EUR 470,604 in bank accounts in Lithuania and GBP 18,198,000 in a bank account in the United Kingdom. In order to trace the assets of the suspects, 1MLA was sent to Switzerland and 1 MLA was sent to Spain. Extensive information was obtained by the Lithuanian Criminal Police Bureau, as an intermediary, through the CARIN network.

Status of the case: The accused who absconded will be prosecuted in absentia in 2019. The seized money will be confiscated.

Conclusion

149. There is now greater awareness among prosecutors and law enforcement officers about the intrinsic value in pursuing ML separately from the predicate offence. As a result, when investigating predicate offences, ML elements are being considered more proactively. The use of parallel financial investigations to identify ML and look beyond the front persons in criminal schemes is gradually gaining ground. Some FIU referrals have successfully been used to initiate ML proceedings (see Box 7.1). However, there are still variations in the approach adopted by the FCIS, the Police and the SIS in prioritising ML offences and their ability to identify and investigate ML. Moreover, most of the cases presented to the assessment team were either at the pre-trial investigation or criminal proceedings stage and have yet to result in a ML conviction. The assessment team is of the view that, despite best efforts, a national ML-specific operational policy would go a long way in ensuring that a more uniform and effective approach is adopted by all LEAs.

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

150. The Long-Term Strategic Action Plan of the Prosecution Service (2013-2023) places the effective investigation and prosecution of organised criminality[54], corruption, financial/economic crimes[55] (which together present the highest threats) and related ML as one of the highest priorities for the law enforcement community in Lithuania. The implementation of the Strategy is monitored regularly. Statistics provided by the authorities in relation to the investigation and successful prosecution of organised crime, corruption and financial/economic crimes indicate that the Strategy is being implemented relatively effectively. As to the consistency of the investigation and prosecution of ML in line with the threats, risk profile and policies, the authorities have only recently started targeting more complex ML cases, involving more substantial sums related to these predicate offences, committed both domestically and outside of Lithuania, as highlighted in boxes 7.1 – 7.4. Some other cases are presented below.

Organised criminality

151. The disruption and dismantling of organised criminal groups has been at the forefront of law enforcement priorities, as evident from the case presented in Box 7.5, which involved over 60 persons. While this is positive, the case also demonstrates that LEAs only started considering pursuing ML at a much later stage of the process and, so far, ML charges have been brought against one person only. The authorities stated that ML investigations against other members of the group are still on-going, before charges could be considered.

Box 7.5: *Organised Crime Group Case*
Predicate crime: The case related to a criminal organised group, involving over 60 persons, which conducted a large-scale cigarette smuggling operation from Lithuania over a wide-spread geographical area, including Lithuania, Latvia, Belarus, the Russian Federation, the Netherlands and Germany. Large quantities of cigarettes from the Russian Federation and the Republic of Belarus were transported through Lithuania to Western Europe, where they were sold. The estimated value of the cigarettes was approximately EUR 11,584,800. In addition, at least 1200 kg of category I precursors of narcotic and psychotropic substances were produced by the criminal group, which generated at least EUR 1,440,000. **Financial investigation:** A financial investigation was conducted in parallel with the investigation of the

[54] Including drug trafficking and smuggling
[55] Including fraud and tax evasion

predicate crimes. In the course of this investigation the funds of the suspects and third parties were frozen; their rights to movable and immovable property were restricted; witnesses were questioned, recognition procedures and covert investigative actions – secret surveillance, monitoring and recording telephone conversations – were carried out. Business and financial activities of some natural and legal persons were investigated. A claim for EUR 6,661,260 in relation to tax evasion was filed in the criminal case due to property damage caused to the state.

Convictions in relation to the predicate crimes: Investigations against 30 persons were conducted separately. Criminal cases against those persons were handed over to courts by using the simplified procedure and subsequently those persons were convicted. Proceedings against 32 other persons charged with almost 150 criminal acts (drug and cigarette smuggling, etc.) are still on-going.

ML charges: Early in 2018, ML charges were instituted against three persons who had also been accused in the main case referred to above. They were charged with seeking to conceal and legitimise property while being aware that it has been derived from crime, transferring the property to other third persons, performing financial operations related to this property and entering into transactions.

Seizure of property (relevance to IO 8): EUR 500,000 were seized, including moveable and immoveable property.

Status of the case: The case is still ongoing.

Fraud

152. Fraud, in various forms, features in the list of ML convictions presented to the assessment team, which is, to some extent, demonstrative of the authorities aligning their efforts with the risks. At the beginning of the period under review, the fraud cases followed a very similar pattern. They involved proceeds derived from bank account fraud, which were then laundered through bank accounts in Lithuania. These cases were relatively straightforward and did not involve significant proceeds. However, in 2016 and 2017, the authorities started pursuing more complex cases, such as the case presented below.

Box 7.6: *Fraud Case*

Predicate Crime: A Lithuanian national acquired various high value properties and money from a number of victims, through the sophisticated use of false documents and fictitious agreements in excess of EUR 1 million. The criminal activity involved fraud, forgery and unlawful activities of a legal entity.

ML element: The proceeds generated by fraudulently schemes were laundered through the bank accounts of different legal entities controlled by the criminal by performing various layering transactions and also through the purchase of real estate property.

Modus operandi: The accused, in order to legalize the property received after the commitment of the above mentioned crimes, knowing that the funds in the company's bank account – EUR 188,253,01, were fraudulently acquired from the victims, organised the management of 6 legal entities and using the bank accounts of these legal entities, carried out financial transactions and concluded purchase-sale contract with the money.

Identification of the case: The ML crime was identified by carrying out a pre-trial investigation of the predicate offence conducted by LEA. A financial investigation was carried out by receiving information from official registers, by accessing bank account detailed information, conducting searches, economic-financial activity and bookkeeping investigation, etc.

Seizure and freezing of money: 1 warehouse, 1 apartment with basement.

Status of the case: final sentence for ML – 3.6 imprisonment, combined sentence (ML + predicate offences) – 7 years 6 months imprisonment.

Corruption

153. The authorities referred to a major corruption-related conviction (2016) involving the financing of a prominent political party in Lithuania using funds of unclear origin: *Darbo Partija* case[56]. In this case, the party systematically received money of unclear origin and used it to support party's activities and election campaigns. It failed to include EUR 7,037,078.91 as income and EUR 3,975,632.30 as expenditures in its accounting books. The leaders of the party were convicted of illegal accounting and tax evasion. The authorities also sought to prove ML but were unable to obtain sufficient objective circumstantial evidence to prove the sources of income due to the following reasons: the illegal income and expenditure of the party were handled only in the form of cash; the main suspects in the case did not cooperate and did not disclose their income sources; the party was particularly careful in concealing the income sources, and would encode them in the documents, e.g. USD 1.6 million from money source "N", USD 900,000 USD from source "X" etc. Upon receipt of information that some of the money intended for the party was transferred to Latvian bank accounts opened by various offshore companies and then cashed out and brought back to Lithuania, MLAs were sent to the Republic of Latvia. The Latvian authorities provided the bank statements of the offshore companies showing that money was indeed transferred to these accounts. However, the persons who actually transported the cash from Latvia to Lithuania could not be identified. The bank accounts of 67 natural persons were examined, over 300 witnesses were questioned, 12 examinations of computer media were carried out by experts and 27 handwriting examinations were carried out. The authorities are of the view that despite the fact that the ML offence was not proven, the conviction of prominent politicians sent out a clear message and had a huge effect on the prevention of unlawful financing of politicians, political activities and corruption in politics. Nevertheless, the authorities concede that the investigation of ML alongside corruption cases needs strengthening.

154. The SIS presented a number of on-going cases where ML related to corruption received considerable attention. They appear to be corruption cases related to public procurement related to abuse of power by government officials. In parallel with these investigations the number of cases of illicit enrichment is also growing (in 2017, 28 pre-trial investigations under art 189[1], 4 cases were referred to the court, in the other cases, the investigations are still pending.). Representatives met on site (including prosecutors) appeared to understand the necessity of pursuing ML in conjunction with corruption. Financial investigations are initiated alongside the pre-trial investigations for corruption. The assistance of the FIU and the FCIS are perceived as very valuable. However, after having viewed closely a number of corruption cases, the assessment team concluded that related ML is not being systematically pursued. The ability of the SIS to extend the investigation of corruption cases to ML elements appears to be still developing. Most of the ML charges were dismissed by the courts, for reasons which are explained under core issue 7.3.

Tax Offences

155. There has been law enforcement focus around ML related to tax offences, especially VAT carousel fraud, common within European Union countries. These cases, such as the one presented in Box 7.7, represent a real effort to pursue the most serious tax-related ML cases.

Box 7.7: *VAT Carousel Fraud case*
Predicate offence: Two Lithuanian nationals operating through domestic and foreign companies purchased lubricant oil, VAT free, from Poland. In order, to avoid paying VAT upon resale, fictitious VAT invoices were

[56] Reference was also made to another corruption case involving a prominent political party; the *Liberalų Sąjūdis* case which is still ongoing.

created alleging that the oil was sold, VAT free, for the amount of over EUR 21 million to companies registered in Latvia, Czech Republic and Estonia, when in fact it was sold in Poland without issuing accounting documents and without paying VAT.

ML: the proceeds generated by the VAT scheme were physically transported from Poland through Lithuania to Latvia. In Lithuania, several persons connected to the scheme performed over 900 transactions from bank accounts of Latvian companies (the alleged buyers of the oil) to the bank accounts of the companies of the two Lithuanian nationals.

Identification of case (relevance to IO 6): The case was identified by the FIU, following the receipt of an STR, which then disseminated the case to the FCIS.

Financial investigation: A financial investigation was conducted in relation to 7 suspected natural persons and over 60 fictitious legal persons. It was revealed that there had been 300 cash transportations and in parallel 900 bank transactions were carried out in pursuance of the scheme.

Seizure and freezing of property (relevance to IO 8): During searches at the suspects' residences, various currencies were found and seized (EUR 1,000,000 in total, out of which EUR 95,700 were found and seized at the border). Freezing orders were imposed on real estate, shares, and money in bank accounts (total value EUR 2,036,258) of the suspects and related legal entities.

Formal and informal co-operation (relevance to IO 2): 16 coordination meetings were held in Poland, between Lithuania and Polish LEAs. A JIT was created with Latvian LEAs (5 meetings were held in Latvia, procedural actions such as questionings, examinations etc. were conducted); 2 MLA requests were sent to Czech Republic, 8 MLA requests were sent to Poland, 2 MLA requests were sent to Estonia, 3 MLA requests were sent to Latvia, 2 MLA request were sent to Hungary, 3 MLA requests were sent to Slovakia and 1 MLA request was sent to Russia.

Status of the case: Criminal proceedings are expected to be instituted in 2019, which will also include ML charges.

ML cases involving transportation of cash at the borders

156. As stated elsewhere in this report, the authorities consider the ML risks related to cash as high due the widespread circulation of cash within the Lithuanian economy and the significant volume of incoming and outgoing formal and informal remittances. It was positively noted that some ML cases involving money mules were identified at the border, such as for instance the case presented below.

Box 7.8: *Money Mules[57] Case*

Predicate offence and ML: Chinese and Vietnamese citizens engaged in trading activities in Poland. The proceeds generated through the illegal trading activities were transported from Poland to Lithuania, by Lithuanian nationals. The proceeds were then transferred from bank accounts held by companies in Lithuanian banks to companies in China against fictitious invoices. In this manner, EUR 20,212,064, USD 18,568,917 and USD 15,300,000 were laundered.

Identification of case (relevance to IO 6): The FIU received information from the Polish FIU indicating that unidentified amounts of cash were transported from Poland to Lithuania. The FIU obtained and analysed data on the companies and persons involved from Lithuanian banks and foreign FIUs. The results of the analysis were disseminated to the FCIS. Procedural coercive measures were used during investigation in order to identify persons in Lithuania who transported the cash and made bank transfers.

Financial investigation (relevance to IO 8): In addition to examining computer equipment, which revealed the suspects' communication by electronic means (over 5, 000 emails), conversations via "Skype" and other programs, numerous bank accounts were analysed. The investigators identified 1,500 bank

[57] Another very similar case was presented which involved the laundering of EUR 20 million.

transfers which were involved in the criminal scheme. It was established that there were 9 offshore companies which had bank accounts in Latvian banks and were used in the scheme of transferring money to China. Also, there were 6 companies registered abroad which had 19 bank accounts in Cyprus and which were used to transfer funds to China. There was 1 company registered abroad which had 2 banks accounts in the banks of the United Kingdom, and there were 6 foreign companies having bank accounts in Lichtenstein, and 1 foreign company having bank account in the Polish bank.

Property seizing and freezing (relevance to IO 8): The prosecutors have restrained the ownership rights of 17 suspects to the real estate, their funds in the bank accounts, cash money found at the suspects' places, funds of offshore companies in the banks of the Republic of Latvia. The total value of the frozen assets amounts to EUR 2,313,987.

Formal and informal international cooperation (relevance to IO 2): 2 MLA requests were sent to Latvia and 2 coordination meetings were held with Latvian LEAs; upon Lithuania's initiative, a JIT (6 meetings) with Latvia was set up with the participation of Eurojust, including Latvia, Poland and Germany. 2 MLA requests and 1 ETO were sent to the United Kingdom, 1 MLA request was sent to Cyprus, 2 MLAs to Poland, 1 MLA to Lichtenstein.

Status of the case: Criminal proceedings are expected to be instituted in 2019, which will also include ML charges.

Conclusion

157. While the authorities have been proactively targeting the predicate crimes which pose the highest threat, they have only recently turned their attention to related ML. Some concrete results have already been achieved in relation to, for instance, organised criminality, fraud and tax evasion, including where the ML is related to foreign predicate offences. However, as acknowledged by the authorities themselves, more efforts are needed in relation to ML-related to corruption. Additionally, while the authorities have already investigated some cases involving the sophisticated misuse of corporate structures and fictitious companies used in trade-based ML, this area needs to be strengthened further as such cases were often cited during the on-site visit by both public and private sector entities as a common typology. ML related to foreign predicates should continue receiving more attention. Few ML cases have been detected at the borders despite the threat posed by the transportation of cash.

Types of ML cases pursued

158. ML prosecutions and convictions have been declining over recent years, as shown in the table below, although the quality appears to have been improving. The percentage of pre-trial investigations that result in criminal proceedings before the courts varies from roughly 20 to 50%. The ratio of indictments to convictions is higher and the acquittal rate (although in the period under review there were 37 acquittals, which is more than the number of convictions) has been decreasing, especially between 2015 and 2017. The large majority of first instance ML judgements are confirmed upon appeal. These figures suggest that there is a tendency by the prosecution service to proceed with the ML charges only where the laundering is investigated alongside the predicate offence and both offences are included in the same indictment. This approach is conditioned by a strict interpretation attributed to the ML offence by the judiciary, as explained below.

Table 14: ML Investigations, Prosecutions and Convictions

Number of ML Investigations, Prosecutions and Convictions

	Pre-trial investigations	Prosecutions	Convictions (first instance)	Convictions (final)
2013	56	12	4	1
2014	60	22	4	4
2015	98	23	15	15
2016	32	14	9	8
2017	21	11	8	5
Total	**267**	**82**	**40**	**33**

159. The table below shows that Lithuania has prosecuted all different types of ML; self-laundering, third party laundering, stand-alone and foreign predicate offence.

Table 15: Number of ML prosecutions per type

Cases	Total number of ML convictions	Self-laundering	Third party laundering	Stand-alone ML	Foreign predicate ML
2013	1	-	1	1	1
2014	4	3	1	1	-
2015	15	11	2	2	-
2016	8	5	2	2	1
2017	5	5	2	3	1
Total	**33**	**24**	**8**	**9**[58]	**3**

160. ML convictions were predominantly for self-laundering (73%) handed down concurrently with a conviction for the predicate offence. The practice to pursue stand-alone ML is not common, even though a conviction for a predicate offence is not necessary to achieve a ML conviction. This principle was first clearly upheld in a 2015 appeal judgement, where the court concluded that in seeking to establish the offence of ML it was not necessary to prove that the offender had committed the predicate offence, establish the circumstances surrounding the predicate offence or define the predicate offence under applicable laws. Prior to the passing of this judgement, the Prosecutor General issued recommendations, in 2013, to clarify the elements required for a successful ML indictment. The recommendations explicitly state that where ML is investigated separately from the predicate criminal act, in the absence of a judgement with respect to the predicate crime due to certain reasons (e.g. death of the perpetrator of the predicate crime, matured statute of limitations, failure to establish the perpetrator of the predicate crime), the criminal origin of the laundered property may be proven on the basis of 'indubitable evidence' that the property was obtained by criminal means and that the perpetrator knew about it.

161. In spite of the 2015 judgement and the recommendations, it was acknowledged that uncertainty persists as to the level of evidence required to convince the judiciary that funds derive from criminal activity. The assessment team was made to understand that there is still a strong degree of resistance within the judiciary to apply the 2015 judgement as a precedent in practice. This was to some extent confirmed in a meeting with the highest representatives of the judicial bench, who stated that, while every case should be decided on its merits, it is unlikely that a ML conviction

[58] All stand-alone ML convictions, except for one, involve third party laundering.

would be achieved absent a conviction for the predicate crime, especially where the underlying criminality has taken place outside of Lithuania. The authorities are confident that some of the most recent cases that are still on-going will reverse this negative trend.

162. It is the view of the assessment team that, while the PG's recommendations have brought some clarity, the requirement to produce 'indubitable evidence' is not clearly explained and it would be perhaps more beneficial to refer to terms such as 'objective circumstantial and indirect evidence'. Additionally, the PG's recommendations do not shed sufficient light on the circumstances under which stand-alone ML may be pursued in cases other than the death of the perpetrator of the predicate crime, matured statute of limitations and failure to establish the perpetrator of the predicate crime. To their credit, LEAs and prosecutors are still willing to put considerable resources into time-consuming and resource-intensive complex stand-alone ML cases with a view to challenging the position of the courts.

163. A review of the nine stand-alone ML convictions (including the 2015 one) reveals that these were straightforward cases, which are not, in fact, representative of laundering where, for instance, the predicate crime and/or the offender is not clearly known. Essentially, they do not test the limits of the ML offence in terms of evidentiary thresholds. Except for two of the cases, they involved the transfer and withdrawal by third parties of funds acquired by another person(s) fraudulently from a victim's bank account. The prosecution was in a position to prove that the funds in question were acquired fraudulently by simply obtaining statements from the victims and the victims' banks. In the other two cases, one involved the conviction of a person who had been previously convicted of a predicate crime and the other the conviction of a third person who had laundered the funds of the predicate offender convicted in a separate but parallel trial.

164. Another challenge which LEAs and prosecutors may sometimes face in investigating and proceeding with ML charges is proving the material and mental elements of the offence. The use of circumstantial and indirect evidence to prove that the launderer knew that the property derived from criminal activity is not always accepted by the courts, although there are clear precedents, as indicated under criterion 3.8 in the TC Annex. Anecdotal evidence suggested that some ML cases where thrown out due to the absence of a confession by the launderer in relation to knowledge that the funds derived from a criminal activity. Additionally, some judges appear to have applied a strict interpretation of the material elements of the ML offence under Article 216 while proving the transfer (change) of character of criminal assets. For instance, in some cases, the court did not consider multiple transfers of funds through various bank accounts to constitute conversion or transfer of property for the purposes of Article 216 and acquitted the accused of the ML charges. It should be noted, however, that on a number of occasions the decisions of the courts have been appealed, which demonstrates that the Prosecution Service has been proactive in challenging such practices.

Effectiveness, proportionality and dissuasiveness of sanctions

165. While a range of sanctions may be applied under Article 216, it is a moot point whether in practice they have been applied effectively and in a dissuasive manner. The assessment team analysed the sanctions for self-laundering and third party/stand-alone ML separately.

166. The table below breaks down the sentences (both fine and imprisonment) for each self-laundering conviction into the sentence for the predicate offence, the sentence for the laundering

offence and the cumulative sentence and allows the reader to compare the sentences with the amount of the funds that was laundered.

Table 16: Break down of sentences (both fine and imprisonment) for each self-laundering conviction

Sanctions for self-laundering convictions								
Year		**Amount laundered (EUR)**	**Sentence for predicate crime (fine) (EUR)**	**Sentence for predicate crime (imprisonment (years. months)**	**Sentence for ML (fine) (EUR)**	**Sentence for ML (imprisonment) (years. months)**	**Combined sentence (fine) (EUR)**	**Combined sentence (imprisonment) (years. months)**
2014	Case 2	16,891.08	1,882	-	5,647	-	3,765	-
	Case 3	27,361.85	3,011	-	5,647	-	3,765	-
	Case 5	170,904.15	7,530.12	1.8	-	1.6	-	2
2015	Case 7	6,319.94	1,883		4,519		4,519.20	
	Case 8	8,433.72	1,506		4,519		3,012	
	Case 9	8,820.09* 3,000**	1,883		2,636.20		2,259.60	
	Case 10	24,581	23,900.5		2,636.20		3,012.8	
	Case 11	68,689.3* 23,991.3**	5,649		11,298		7,532	
	Case 12	4,720.81	6,636.2		4,519		3,012.80	
	Case 13	20,499.29	1,883		4,519		3,012	
	Case 14	4,416	1,883		5,649		3,766	
	Case 15	8,312	3,008		5,640		3,760	
	Case 16	35,681	1,900		5,130		3,420	
	Case 18	2,722	7,155		11,298		7,532	
2016	Case 20	170,000	10,168.2		24,479		6,024.60	
	Case 22	8,370* 6,668**	3,012.8		4,519.2		3,012.80	
	Case 23	444,277.11		3		1.6		2.8 suspended for 3
	Case 24	7,423.16		1.8		2	2,636.2	3.6
	Case 25	14,000		1		1		1.3 and 16 days
				1.8		1		1.6 suspended for 2.6

2017	Case 27	188,253.01		4.4		3.6		7.6
	Case 28	4308** 22,000*		2.6		3		3 suspended for 2
	Case 29	10,517,336.4		6		4		7.9
				2		2		3 suspended for 3
				5.3		4		5.6
					112,980 *			
	Case 30	161,382,14		3		3		4 suspended 2
				2.3		2		3 suspended 2
				1				
				2		2		2.6 suspended 1
				2.6		2		3.6 suspended 2
	Case 32	20,188.93	2,259.6		3,012.8		3,012.8	

* Proceeds generated

** Proceeds laundered

167. Until 2016, all sentences, except for one, consisted of fines averaging EUR 3,500. In most of these cases, the fine imposed for the ML offence exceeds the fine for the predicate offence. The cumulative sentence is almost always lower than the two sentences combined. More importantly, in the vast majority of the cases, the cumulative sentence is significantly lower than the laundered amount (e.g. case 2, 3, 10, 11, 13). For instance, in case 20, the accused was fined EUR 6,024.60 despite the fact that he was convicted for laundering EUR 170,000 and the individual fines for the predicate offences and the ML were EUR 10,168.2 and EUR 24,479 respectively. While few of the cases in the period 2013-2015 involved serious ML offences judging by the volume of laundered assets, the assessment team still finds that these sanctions are far from being proportionate, dissuasive and effective.

168. Since 2016, the imprisonment sentence appears to have found more favour among the judiciary. This shift coincided with a positive development in relation to the cases put before the courts by the prosecution, which involved significant amounts of laundered funds deriving from more serious underlying predicate offences (e.g. carousel fraud and prostitution). In most cases, the sentence for the predicate offence is higher than for the laundering (e.g. case 23, 27, 29). The cumulative sentence is often lower than the two combined. In more than 50% of the cases, the sentence is suspended. Generally, imprisonment sentences appear to be on the lenient side. For instance, in case 23, having misappropriated company funds, the accused laundered EUR 444,277.11. The sentence for the predicate offence was 3 years, for the ML 1.6 and combined he received a sentence of 2.8 years imprisonment suspended for 3 years. It is difficult to conclude that these sentences have had the effect of dissuading criminals from laundering their ill-gotten gains. The Prosecution Service expects that the situation will improve as a result of a change in the CC which will not enable the courts to suspend a sentence where a person is convicted of a serious crime (which includes ML).

* proceeds attempted to be laundered

* conviction of a legal person

169. Turning to third party and stand-alone ML convictions, a similar picture emerges, as evident from the table below.

Table 17: Sanctions for third party and autonomous ML convictions

		Amount laundered (EUR)	Fine(EUR)	Imprisonment
2013	Case 1	7,450	3,765.06	-
2014	Case 4	261,533.83	11,295.18	-
2015	Case 6	885.08	225.96	-
	Case 17	202,734	4,519.20	1 suspended for 2
2016	Case 19	4,300	225	-
	Case 21	89,969	20,713	-
2017	Case 26	4,900	828	-
	Case 31	4,000	2,485.52	-
	Case 33*	16,000	7,532	4 suspended for 3

170. Most of the sentences for stand-alone ML (all of which, except for case 33, were third party laundering) consist of fines. The fine is always lower than the sums that were laundered, in some cases significantly lower (case 4, 21). The only two imprisonment sentences that were imposed were suspended. It is also difficult to identify any patterns in these cases. Cases 4 and 21, where the sums laundered were significant, only attracted a fine, whereas case 33, where the funds involved were much lower resulted in a fine and an imprisonment sentence (albeit suspended). The assessment team does not consider these sanctions to be dissuasive and effective.

171. In the period under review, the prosecution service instituted criminal proceedings for ML against nine legal persons. There has only been one ML conviction for a legal person, which received a fine amounting to EUR 112,980. It is not clear what the involvement of the legal person was. Considering that legal persons feature recurrently in the cases presented by the authorities, more ML convictions would have been expected.

Extent to which other criminal justice measures are applied where convictions is not possible

172. There have been cases where, following an investigation into ML, the Prosecution was not able to institute criminal proceedings for justifiable reasons, cited by the authorities as including unsuccessful mutual legal assistance, missing persons, unclear subjects, unclear transactions, fictitious enterprises and transactions, etc. In these cases, the authorities have successfully pursued the confiscation of the laundered proceeds on a non-conviction basis by applying the conditions under Article 94 of the CPC. The first case of this nature was decided in 2013, which served as a precedent for two other cases were started in 2016-2017 and completed in 2018: more than EUR 17 million was confiscated in this manner. These cases are now serving as a reference for LEAs to actively seek the transfer of funds into the ownership of the state where they are not in a position to prove ML but one or more of the following conditions exist: the origin of funds is unclear (when there are reasonable doubts to believe that their origin is unlawful), no person makes an ownership claim on the funds and the presumption of good faith in relation to the funds is not proven.

Conclusion

* laundering of funds generated by the predicate offender

173. **Lithuania has achieved a moderate level of effectiveness for IO 7.**

Immediate Outcome 8 (Confiscation)

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

174. Depriving criminals of proceeds of crime is a policy issue endorsed at the highest levels within the prosecutorial and law enforcement structures in Lithuania. More efficient application of asset recovery and extended confiscation are stipulated among the priorities addressed by a national long-term strategic plan.[59] The legal framework governing seizure and confiscation is extensive and includes confiscation of the laundered property, both direct and indirect proceeds of crime, property of equivalent value and property in the hands of third parties. It goes further than the FATF Standards as it allows for extended confiscation and Lithuania's version of non-conviction-based confiscation under Article 189[1] of the CC (unjust enrichment).

175. At the operational level, the General Prosecutor issued various binding recommendations to implement the seizure and confiscation-related elements of the strategic plan. Foremost among them are the recommendations on Financial Investigations, which, *inter alia,* require the compulsory initiation of a financial investigation alongside a criminal investigation in relation to crimes which generate material gain. A handbook for practitioners (Methodology on Asset Investigation) was issued to complement the recommendations. All representatives of LEAs and prosecutors met on-site were aware of the recommendations on financial investigations and understand their significance. The General Prosecutor has succeeded in instilling a culture which accentuates the merits of financial investigations. However, this notion appears to have gained significant traction closer to the on-site visit and the complexity and sophistication of financial investigations are still developing, with some significant success being registered already.

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

176. Since the previous evaluation round, there has been tangible progress in the implementation of confiscation-related requirements. There is a stronger appreciation of the need to identify, trace and seize proceeds of crime and instrumentalities at the earliest stage of an investigation to secure future confiscations. Recently, provisional measures have become more embedded within the operations of pre-trials LEAs.

Financial Investigations

177. Financial investigations are initiated in relation to every proceeds-generating crime. Where the material gain does not exceed EUR 1,500, only a simple financial investigation is required. The purpose, in these cases, is to identify the property that could potentially be subject to confiscation. Otherwise, a fully-fledged financial investigation is compulsory. Where there are no indications that a proceeds-generating crime has taken place, but there is information indicating that a person who has

[59] Public security Development Programme 2015-2025, Chapter III Goals and tasks of the Programme criteria for evaluation of the evaluation of Programme Implementation and their Values:
45.2.3. to increase the effectiveness of the mechanism for the search, seizure and confiscation of property received by crime;

no official source of income has conducted certain transactions exceeding EUR 25,000, a financial investigation is also required. This is also the case where during the application of coercive measures or a search by LEAs money in excess of EUR 25,000 is found or seized or where a person has not declared income amounting to EUR 25,000 or more.

178. The PG's Recommendations distinguish between financial investigations during the criminal intelligence stage and the pre-trial stage. The scope of the financial investigation differs and as noted under IO 6, the content of the investigation during the criminal intelligence stage focuses to a large extent on whether (1) the suspect has failed to declare income to the STI; or (2) the suspect is in a position to prove that the income sources were lawful, and, if not, whether elements of the offence of unlawful enrichment (Art 189[1] CC) could be established. The consequences are outlined under IO 6 and 7.

179. Financial investigations during the pre-trial stage are regularly carried out alongside the investigation of the predicate offence. LEAs may request the BoL, FIs, credit institutions and any other legal person to furnish information on economic and financial operations of a natural or legal person and information on the use of financial instruments and means of payment. This power appears to be used routinely by LEAs. Although no statistics are maintained, the FIs met on-site confirmed that they receive LEA requests on a daily basis. This type of request has grown exponentially in recent years, with some of the larger banks indicating that an entire unit has been set up internally, specifically to manage the flow of information with LEAs. This suggests that LEAs have become increasingly conscious of the value that financial information brings to an investigation. The assessment team was also satisfied that LEAs regularly access various information databases[60] which they have direct/indirect access to, including requests sent to foreign counterparts through informal channels.

180. At the beginning of the reporting period, up until 2016, the emphasis of financial investigations appeared to be on developing the financial profile of the suspect, rather than (1) tracing the proceeds of crime and other property that may become subject to confiscation; and (2) identifying the extent of criminal networks and/or the scale of criminality. This was likely linked to the absence of a 'follow the money' approach starting from the intelligence stage. Additionally, the PG Recommendations on Financial Investigations, as they stood at the time of the on-site evaluation, focussed on the property belonging to the suspect and did not extend to property that might have been passed on to third parties.

181. As a result of experience gathered over the years, the sophistication of financial investigations has improved (see case examples provided under IO 7), to the extent that at the time of the on-site visit, advanced discussions were being held at the Collegiate Council of Prosecutor General's Office (the supreme body within Prosecution Service) to significantly update the Recommendations on Financial Investigations. While the law enforcement officers conducting the investigation of a predicate offence conduct financial investigations simultaneously, they may be supported on request by two specialised units (one situated within the FCIS and the other within the Police) with expertise on financial analysis and forensic accounting. As mentioned under IO 7, it has become common to form joint investigation teams comprising intelligence officers, case investigators and financial specialists, when investigating complex crimes. However, the skills and knowledge of all LEAs and prosecutors at all the stages of the seizure and confiscation process should be improved further.

[60] To include list

Volume and type of seized and confiscated assets

182. The authorities presented the following table which contains aggregated data on the volume of seized and confiscated property in relation to ML and other predicate offences. It also includes data on cash seizures, restitution to victims, which is not included in the data under confiscated property and data on the value of seized goods (to provide a more holistic picture).

Table 18: Volume and type of seized and confiscated assets

	2013	2014	2015	2016	2017	Total
Seized Property (predicate offences)(EUR)	13,121,158	76,115,984	14,970,554	108,674,324	17,167,482	230,049,502
Seized cash	884,128	237,418	84,107	368,560	529,669	2,103,882
Seized Property (ML)(EUR)	3,253,940	105,000	52,130	-	315,848	3,726,918
Confiscated Property (predicate offences)(EUR)	-	-	-	425,500	2,488,509	2,914,009
Confiscated Property (ML) (EUR)	2,317	-	2,722	21,953	11,367,190	11,394,182
Restitution to victims (EUR)	2,487,012	2,506,406	2,066,835	3,792,181	2,091,936	12,944,370
Value of seized goods (EUR)	7 180 104	4 157 766	4 239 867	1 509 957	2 269 904	19 357 598

183. The table provides a clear indication that the implementation of seizure and confiscation mechanisms has improved considerably in Lithuania, especially when compared to the situation at the time of the 4th Round MER in 2012. However, although the volume of seized assets has increased significantly, the confiscation results remain somewhat modest. While the representatives of LEAs and prosecutors met on-site were very keen to demonstrate that depriving criminals of their proceeds has become a fundamental aspect of their activities, they were in unanimous agreement that there is no room for complacency and further improvements are needed. In particular, they are acutely aware that, as their efforts in pursuing the most serious proceeds-generating offences intensify, a more systematic approach to seizure and confiscation should be adopted and additional technical and human resources should be allocated to the area of financial investigations. They acknowledge that the confiscation results over the entire period under review could have been higher but are also confident that the figures will increase significantly in the very near future, given the amount of property that is currently seized as part of ongoing investigations.

184. In addition to the figures above, despite the termination of an investigation into ML in three separate cases (1 in 2013 and 2 in 2018), the total amount of approximately EUR 17 million was forfeited in favour of the state based on a prosecutorial decision in terms of Article 94 of the CPC, which regulates the disposal of property when terminating criminal proceedings or a judgement is rendered. In these cases, the funds, which had been seized during the investigation, were transferred to the state since their origin could not be established and no ownership claim was made in their regard.

185. The judiciary confirmed that all types of confiscation orders have been made in practice, except for indirect proceeds and laundered property. Case examples show that property from foreign

proceeds has been confiscated or at least seized (see for instance Box 7.1 and 7.8). According to the practitioners the use of the confiscation of equivalent value is not uncommon, although no practical examples were provided. In those cases where property is transferred to a third person, in terms of evidentiary thresholds, the accepted judicial practice is to prove at a minimum negligence on the part of the person receiving the property. There is limited experience in the confiscation of co-mingled property. Similarly, there were no cases of seizure and confiscation of instrumentalities intended for use. However, the practitioners were quick to point out that, despite the fact that the legal framework does not explicitly cover the confiscation of such instrumentalities, the use of ancillary offences, particularly 'attempt' and 'preparation' would be sufficient to legally remove such items from the possession of the offender.

186. There is a universal understanding that property as defined in the CC covers all types of property listed in the FATF Methodology, including virtual currencies, which are considered to carry economic value rather than simply constituting electronic data. Practical examples were presented to the assessment team on the seizure and confiscation of virtual currencies. For instance, in 2017 when conducting procedural actions based on a MLA request, funds were seized (by restricting access codes) in virtual currency and crypto-currency wallets, hosted on a server, as well as in other servers rented for the same purpose and having the same IP address. The seizure of the property right is currently still in force.

187. In relation to grand corruption cases, the SIS has developed the ability of proving the criminal property based on favour-to-favour type of corruption conduct, even where the object of the bribe is not a material advantage. While the SIS conducts financial investigations, it does not yet have a very strong culture of following the money in corruption cases.

188. The application of extended confiscation is still rare as a result of two objective reasons. Article 72^3 of the CC came into force on 10 December 2010, which means that its provisions only apply to property acquired after this date. This has hindered its practical application in the many cases that LEAs were investigating in the period under review. Additionally, extended confiscation is closely linked to and became effective at the same time as Article 189^1 of the CC, whose constitutionality was challenged before the courts. The matter was resolved on 15 March 2017 by the Constitutional Court, which concluded that the criminalisation of unlawful enrichment does not contradict any of the fundamental human rights enshrined by the Constitution of Lithuania. Prior to that, the application of Article 189^1 was held in abeyance, which had a chilling effect on the application of Article 72^3, given their links. At the time of the on-site visit, both articles were under renewed scrutiny by the Collegiate Council of the Prosecution Service to establish mechanisms and develop recommendations for their effective implementation.

189. As for the confiscation of proceeds outside of Lithuania, the authorities stated that MLA requests are sent to foreign states where a financial investigation indicates that funds were transferred from Lithuania. The case provided under Box 7.8 is a good illustration of the proactive stance taken by the authorities in seeking to trace and seize assets that have left the country. Other similar cases were presented to the assessment team. Although the legal system does not present any impediments as far as repatriation of confiscated proceeds of crime to third states is concerned, repatriation in the domestic context is not developed.

190. There are no shortcomings within the legal framework governing provisional seizure measures which hinder their effective application. In practice, applications by the prosecution for restraint of assets have never been rejected by the courts. This was confirmed by the representatives of the

judiciary met on-site. The practical application of Article 151 CPC on provisional restraint of ownership rights is broadly elaborated within the PGO recommendations. The basic precondition for seizure is to prove or establish the circumstances that prove that material benefit has been gained. The tracing for such property is conducted by means of financial investigations through procedural coercive and non-coercive measures, such as requests for information to FIs. A very positive aspect which directly impacts on the effectiveness of the system is the existence of a bank account register available for all LEAs (direct) and prosecutors (indirect). Searches are also used in the identification and tracing of assets. During such searches, the cash and other moveable items are seized, whereas ownership to other valuable items (e.g. works of art) may be subject to restraint of ownership rights, pursuant to prosecutor's decision. In cases when data about the property is kept by other persons or registered in the name of other persons, information is obtained by means of wiretapping and surveillance. In cases where it is established that the property has been transferred on the basis of fictitious transactions, the ownership right to such property is restricted with a view to secure its probable confiscation, provided that there are grounds to presume that this property has been acquired using funds of criminal origin or as a result of unlawful enrichment. If no criminal origin of the property is detected and if there is no basis to open a pre-trial investigation into criminal offence under Article 189^1 of the Criminal Code (unlawful enrichment), information is handed over to the tax administrator to make a decision regarding tax violations. All necessary information, including particular sources and procedural measures to apply provisional restrain of ownership rights are described in the PGO's Recommendations.

Management of seized and confiscated property

191. While the approach to the management of seized assets is fragmented (see criterion 4.4), it appears to work effectively in some cases. The authorities referred to some examples of management of assets under seizure, such as airplanes and vehicles, which are at risk of deterioration or devaluation. However, no examples were provided in relation to management of, for instance, going concerns (e.g. the management of a profitable company trading in goods to ensure that it does not lose value). The assessment team is of the view that the establishment of an asset management office will be inevitable should Lithuania continue improving the system for the seizure of property, which is already resulting in the seizure of significant volumes and different types of assets. The authorities indicated that a group of experts has been established to assess whether seized assets are being adequately managed. Additionally, Recommendations of the Prosecutor General on the realisation of seized property in the stage of pre-trial investigation are being prepared for implementation in 2019. Furthermore in 2018, the Prosecutor General's Office put forward proposals to the Ministry of Justice on the establishment of such competent authority, in order to strengthen asset management functions.

Enforcement of confiscation orders

192. The responsibility for the execution of confiscation orders is divided between bailiffs and the STI. Complete statistics on the enforcement of confiscation orders are missing (the Chamber of Bailiffs does not collect any statistics and statistics from the National Court Administration are not sufficient). The assessment team, therefore, could not come to a conclusion on the proportion of criminal assets which are effectively confiscated. Generally, bailiffs are responsible for the identification and tracing of property subject to confiscation to ensure its forfeiture. The STI is responsible for converting confiscated property into money (in terms of volume not exceeding EUR 17,500 this is sub-contracted to private entities) to be transferred into a compensation scheme or

directly to the state budget. Funds derived from confiscated property are transferred to the ownership of the state. It is not specifically used for the needs of LEAs. Both bailiffs and the STI have adequate operational powers. The assessment team was satisfied that both have the capacity to fully execute all kinds of confiscation orders. However no practical examples have been provided to date. The assessment team harbours some doubts in relation to the execution of confiscation orders in practice. There appear to be no practical procedures in place to govern the activities of bailiffs in terms of execution of enforcement orders. For instance, no procedural guidance is available on how to identify property in complex situations.

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

193. The Customs Criminal Service does not appear to have an extensive ability to identify non-declared cash and false declarations due to a shortage in human and technical resources. The Customs explained that whenever a person makes a declaration no further action is undertaken to determine whether the cash may be related to crime. Additionally, the Customs do not generally stop or restrain cash for a reasonable period of time to ascertain whether evidence of ML/FT or other predicate offences may be found. Customs officers do not receive training on ML indicators and do not have access to certain databases, such as the PNR, which would facilitate their work. The absence of a comprehensive framework raises significant concern given the wide circulation of cash and the ML/FT risks it poses in Lithuania. It is clear from the statistics below, that the amounts restrained at the border have been limited, especially when compared with the very large volume of money transported in and out of the country as explained in chapter 1 under the section on materiality. The system works to some extent and the authorities have managed to secure a conviction for the smuggling of cash in 37 cases. However, the volume of confiscated cash (EUR 554,871 over a period of five years) is low. Additionally, the authorities recognise that the cases of cash smuggling should have been investigated further to identify possible ML elements. Lithuania ought to strengthen the criminal intelligence potential in identifying the money transportation routes, persons and schemes, especially between the inner borders of Lithuania with Latvia and Poland, and within the non-EU borders.

Table 19: Falsely or undeclared cross-border transactions

Year	Non-declarations	False declarations	Assets restrained (amount in EUR)	Total number of criminal cases (crossing of State borders)	Amounts of cash identified (total amounts in EUR)	Convicted persons	Amount confiscated (total amount in EUR)
2012	7	6	758, 697	7	EUR 272,130	6	EUR 223,581
2013	5	5	221, 707	3	EUR 52,720	2	EUR 6,478
2014	10	-	267, 932	10	EUR 267,943	9	EUR 184,474
2015	7	1	782, 065	6	EUR 102,247	5	EUR 74,738
2016	5	1	103, 049	5	EUR 102,600	5	EUR 65,600
2017	6	-	390,129	6	EUR 390,129	6	-
In total:	40	15	2 523 579	37	EUR 1,187,1769	32	EUR 554,871

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

194. Information provided by the authorities suggests that generally proceeds are confiscated in line with the predicate crimes identified as higher risk, and in line with Lithuania's policies and priorities. For instance, a significant volume of assets has been seized over a five year period (over EUR 230 million) in relation to organised crime and financial/economic crimes, such as fraud, VAT carousel cases and other tax-related crimes, which constitute the highest threats in the country. This dovetails with the Long Term Prosecution Strategy (referred to under core issue 7.2) which aims to repress such crimes by depriving criminals of their ill-gotten assets. This matter is of particular significance in the context of Lithuania's fight against organised criminality. There has not been a lot of progress in relation to corruption offences, in terms of seizure and confiscation. It is also very positive that Lithuania has its sights on developing technologies, such as virtual currencies, which shows that the objectives of the authorities are capable of evolving in line with emerging risks. However, the results in relation to actual confiscation are still rather modest and further efforts are needed in relation to all proceeds-generating crimes and confiscation of cash at the borders.

Conclusion

195. **Lithuania has achieved a moderate level of effectiveness for IO 8.**

CHAPTER 4. TERRORIST FINANCING AND FINANCING OF PROLIFERATION

Key Findings and Recommended Actions

Key Findings

Immediate Outcome 9

1. The authorities involved in the prevention and investigation of FT and terrorist-related crimes have a broad understanding of FT risks and threats, which is consistent with the level of risk present in the country. The SSD has the most advanced understanding of FT risks.

2. There have only been two FT cases in Lithuania. One resulted in a FT conviction. The other is still on-going. There have been seven terrorism related investigations. No financial investigations were carried out alongside these investigations.

3. While there appear to be mechanisms in place for the identification, investigation and prosecution of FT, the skills required to deal with such cases need to be developed further.

4. The Customs Service does not have the specific power to stop and restrain currency at the borders in order to ascertain whether evidence of ML/FT may be found. In addition, MVTS providers may not be submitting relevant FT suspicions. Both of these circumstances may result in the non-detection of FT.

5. While the Public Security Programme (2015-2025) contains a specific goal relating to terrorism and FT, it does not appear that an action plan has been developed to implement this goal in practice. Therefore, the assessment team could not determine that the investigation of FT would be integrated, and used to support, national counter-terrorism strategies and investigations.

6. The sanctions provided in the CC for FT offences appear to be proportionate and dissuasive. In the one court decision related to FT the most severe punishment was applied. The instrument of the crime was confiscated.

Immediate Outcome 10

1. The legal framework governing targeted financial sanctions ("TFS") for FT is not fully in line with the Standards. The implementation of TFS has technical and practical deficiencies due to the procedures set at the EU level that create delays on the transposition of UN designations.

2. Although no assets or funds subject to freezing have been identified up to date, which is consistent with Lithuania's current FT risk, the country displays elements of an effective system to implement TFS pursuant to UNSCRs 1267 and to UNSCR 1373. Banking institutions are aware of UN and EU designations and have systems in place to monitor customers and transactions against the UN, EU and other national lists. The DNFBPs' sector in general demonstrated limited understanding of their TFS obligations. The representatives of Fintech sector appear to be aware of their obligations stemming from the sanction regimes.

3. Lithuania does not have a mechanism(s) to identify targets for designations and has not proposed or made any designations. The operational framework governing the implementation of TFS among the authorities lacks clarity.

4. Although the authorities use a broad range of tools to engage in TFS-related communication with REs (e.g. dedicated space on TFS on their websites and responding to telephonic queries) outreach provided through annual trainings is mostly provided to banks and is not sufficiently focussed on TFS-related matters.

5. Potential vulnerabilities within the NPO sector and cash-related FT indicators were taken into account during the NRA exercise and the FIU Strategic Analysis.

6. Most of the mitigating actions related to NPO risks set in the NRA Action Plan had not been implemented or they were underway.

7. No formal guidance, outreach or training on FT risks to NPOs or donor communities by the authorities has been carried out during the period under review. All NPOs met on-site were unaware of their obligations and the possible abuse for illicit activities including FT.

8. The Register of Legal Entities ("RLE") contains information that is publicly available[61]. However, the RLE database does not provide for full-scale demographic information such as origin and types of activities of NPOs.

Immediate Outcome 11

1. The legal framework governing targeted financial sanctions for PF is not fully in line with the Standards. The implementation of TFS has technical and practical deficiencies due to the procedures set at the EU level that create delays on the transposition of UN designations.

2. While no funds related to PF have been frozen, awareness of PF-related TFS is widespread among banks. In many cases banks demonstrated a strict approach in complying with TFS. There were instances where banks refused payments which were not subject to international sanctions (e.g.

[61] http://www.registrucentras.lt/jar/p_en/

banks flag transactions with regard to Iran). Awareness of risks in the non-financial sector is generally limited to awareness of lists and seemingly sporadic screening against them.

3. The MFA is the lead agency for countering PF. Although there is no interagency mechanism to resolve issues related to PF, a weekly coordination meeting on policy issues takes place at the ministerial level. The Investment and Export Department of the Ministry of Economy (MoE) is the licensing Authority for dual-use goods. The MoE regularly holds workshops for industry associations to notify them of updates concerning licencing and updates of lists and sanctions. Both the FIU and the MFA have adopted a more targeted approach in assisting banking institutions to comply with their TFS obligations related to PF. Other supervisors exhibited limited understanding of risks entailed by sanctions evasion.

Recommended Actions

Immediate Outcome 9

1. Financial investigations should be carried out in parallel with terrorism and other related cases (e.g. smuggling of firearms) with a view to identifying and investigating FT. The PG should develop recommendations for financial investigations in relation to FT.

2. In order to increase the capabilities and capacities of Lithuanian agencies to identify, prevent and combat the more recent trends and methods of FT, practical mock case training should be periodically conducted jointly by LEAs engaged in FT investigations.

3. The SSD should share its knowledge of FT issues with the Prosecution Service, other LEAs and the FIU to ensure that there is an even level of understanding of FT risks among authorities.

4. Authorities should review their practice of terrorism related investigations and prosecution with a view to ensuring that investigations and convictions in terrorism and FT cases are carried out promptly.

5. Border cash control mechanisms should be strengthened by providing a legal basis for the possibility to administratively stop and restrain terrorism and FT suspects' assets, and by continuing developing typologies and indicators to support the identification of such assets.

6. The Prosecution Service and the Police should develop operational policies to implement the third goal of the Public Security Programme (2015-2025) dealing with terrorism and FT, to ensure that FT investigations would be integrated, and used to support, national counter-terrorism strategies and investigations.

Immediate Outcome 10

Lithuania should:

1. enable targeted financial sanctions relating to FT to be implemented without delay, in line with the FATF Recommendations;

2. introduce a mechanism(s) for the identification of targets for designations;

3. ensure that all FI and DNFBP supervisors understand the risks entailed by sanctions evasion and adequately supervise and monitor that PF-related TFS are applied immediately;

4. expeditious and systematic dissemination of the UN sanctions lists to all REs is required.

5. adopt a proactive communication strategy towards all REs on FT-related TFS (targeted trainings, workshops and guidance by all supervisory authorities is required).

6. strengthen the next iteration of the of the NPOs review by the FIU;

7. include representatives from the NPO sector in the next NRA process when assessing the FT risk of the sector;

8. conduct targeted outreach activities to the NPO sector regarding the FT risk, advise them of best practices to protect themselves, and conduct on-going monitoring of NPOs at risk;

9. implement all the mitigating actions set in the NRA Action Plan.

Immediate Outcome 11

Lithuania should:

1. ensure that targeted financial sanctions relating to PF are implemented without delay;

2. establish a national mechanism for the coordination and implementation of policies and strategies to combat PF;

3. ensure that all FI and DNFBP supervisors receive appropriate training, understand the risks entailed by sanctions evasion and adequately supervise and monitor PF-related TFS;

4. provide guidance to obliged entities specifically on the implementation of the PF-related TFS regimes;

5. conduct further awareness-raising activities in order to enhance the knowledge and understanding of the private sector on PF-related TFS obligations;

Immediate Outcome 9 (TF investigation and prosecution)

196. The key players within the CFT framework are the SSD, the Criminal Police Bureau, the FIU and the Prosecutor General Office. All agencies demonstrated an understanding of FT risks and have broad powers to obtain financial intelligence and other information required for FT investigations. The SSD and the Police are authorised to carry out criminal intelligence investigations. The Police is responsible for conducting FT pre-trial investigations. The PGO supervises and controls the lawfulness of criminal intelligence actions and pre-trial investigations. In complex cases, the PGO may conduct pre-trial investigations itself, with the assistance of the Police. This has been the case for all terrorism and FT pre-trial investigations that have taken place so far in Lithuania.

197. The NRA concluded that the FT threat level is low in Lithuania. No signs of terrorism-related activities have been detected. In particular, no activities of radical Islamist terrorist organisations, no threats of terrorist attacks or departures of nationals to the Syrian and Iraq conflict areas have been identified. Nevertheless, it was concluded that, hypothetically, being a member state of the EU and NATO, Lithuania is a potential, though not a priority, target for Islamist terrorists. The level of radicalisation has remained low within the Lithuanian Muslim community. The terrorism threat situation in Lithuania is partly and indirectly dependent on European terrorism trends. In the short-term, the threat of terror attacks planned by ISIS and individuals in Europe supporting its ideology will remain high. With the defeat of ISIS in Syria and Iraq, some of its members may attempt to return to Europe by using the routes of irregular migrants. However, apart from some unconfirmed suspicions in the form of intelligence information, no evidence was found by Lithuania indicating that

Lithuanian residents or non-residents have travelled to conflict zones abroad from or through Lithuania to help foreign terrorist groups or financed terrorism.

198. According to the NRA, independently-planned terrorist acts requiring small funds and carried out by individual extremists (lone wolves) constitute an emerging terrorist and FT threat in the EU and other Western countries. The authorities consider that Lithuania could be a base for planning attacks in other European countries, although this scenario has not been supported by any concrete indication at this stage.

199. The authorities defined the following possible external factors that may have effect on the level of FT risks to Lithuania:

- international terrorism;
- Islamist propaganda activities on the Internet;
- radicalisation trends in EU countries;
- illegal migration to Europe; and
- Lithuania's Schengen Area membership, which could make the country a transit state for terrorists on their way to conflicts areas in Syria and Iraq.

200. Actions to counter the terrorism/FT threat were also defined:

1. monitoring of radicalisation;

2. monitoring of migration processes, especially from terrorism sensitive regions (including in processing the applications of asylum seekers relocated from Greece, Italy and Turkey); and

3. international cooperation.

201. Although the assessors consider that the NRA includes limited information on FT risks (limited focus on financial instruments that are most risky from the point of view of FT, distribution of risks into three categories – collection, movement, usage), the agencies met on-site demonstrated a significantly more advanced understanding of FT risks. The most knowledgeable authority in this sphere is the SSD. All representatives met on-site agreed that the major FT risks are posed by the "lone wolf" phenomenon, cash border movements, abuse of NPOs (in particular religious NPOs) and the presence of individuals and organisations supporting terrorist activities. Hypothetically, in their view, in addition, financial instruments such as virtual currencies and money remittances, as well as the use of corporate structures, may also pose a certain level of risk. Broadly, these risks are understood by all agencies, and investigators, prosecutors and intelligence officers appear to have the necessary skills and knowledge to identify, investigate and prosecute FT, should the need arise. Nevertheless, some prosecutors pointed out that recent cases of ML related to large amounts of cash smuggled from abroad, highlight the need for more vigilance at the border, as the same typology could be used in the context of FT. They consider the non-dissuasive nature of sanctions in relation to undeclared/falsely declared movement of cash and the absence of a mechanism to trace the possible criminal origin of such cash when detected as factors which could increase FT risks.

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

202. The PGO is responsible for supervising investigations and conducting prosecutions into FT. In accordance with the Recommendations of the Prosecutor General on Specialisation, there is a

separate specialisation for crimes against public safety (which comprises FT crimes defined under Article 250(4) CC) situated within the Department for Organised Crimes and Corruption Investigation of the Prosecutor General's Office and in specialised Organised Crime and Corruption Investigation Divisions of regional prosecutors' offices. A prosecutor has also been appointed at the Prosecutor General's Office with a specialisation in the field of terrorism crimes. Due to the complexity of terrorism and FT cases, the prosecutors conduct the investigations themselves with the assistance of the Police.

203. There have been one prosecution and conviction for FT. The case was opened in 2007, prior to the evaluation period. The case related to the terrorist group "The Real Irish Republican Army" operating in the Republic of Ireland and in the United Kingdom. The case was referred to the criminal courts in 2009. Having gone through all judicial stages, including the court of cassation (final appeal), the case became final on 14 April 2017, resulting in a FT conviction.

Box 9.1

On 8 October 2007 a pre-trial investigation into support to a terrorist group and other crimes was launched. Weapons had been purchased by non-residents in Lithuania to be used for terrorist purposes. EUR 100,000 were allocated to acquiring and smuggling armaments by suspects. It is not clear whether this amount was eventually used and what the source and movement of these funds were.

In 2008 one suspect was arrested and other three were identified as suspects. A search was announced and European Arrest Warrants were issued accordingly. The search was carried out at the place of residence of the suspects. In order to gather the necessary evidence, the LEAs and the prosecution service of Lithuania cooperated with relevant agencies of Ireland, the UK and Spain, to co-ordinate covert actions.

On 10 March 2009, a decision was taken to conduct proceedings against M. C. (the original suspect) separately and charges were filed before the criminal court. M.C. was convicted for FT (Art. 250^4(1)), for which he received a custodial sentence of 5 years, 8 months and 11 days. For the attempt to dispose of firearms, ammunition, explosives (Art. 22(1), 253(2) of the CC) he received a custodial sentence for 4 years and 6 months. For the preparation to smuggle firearms, ammunition and explosives (Art. 21(1), 199(1) of the CC) he received a custodial sentence of 5 years and 6 months. In accordance with Art. 63 (1), 63(2), 63(5)(1) of the CC M. C. received the final consolidated sentence of imprisonment for 5 years, 8 months and 11 days. In addition, the instrument of the crime was confiscated, i.e. EUR 17,250.

During the same period Ireland decided to extradite the three other suspects. One of them died and the investigation on this person was terminated on 16 March 2010. One of the other suspects was arrested in the UK. The UK refused to extradite this person to Lithuania. Subsequently, Ireland refused to extradite the third suspect. Currently, the LEAs of Ireland are dealing with the extradition of the suspect who has returned from the UK to Ireland. As soon as the Irish LEAs make that decision, the Lithuanian LEAs will decide on whether to institution criminal proceedings. Should the extradition process be unsuccessful, proceedings will be conducted in absentia.

204. It is difficult to conclude whether the results achieved in the period under review are consistent with the country's risk profile in the absence of a significant number of prosecutions and convictions. However, in light of the fact that no information exists which suggests that Lithuania faces an elevated risk of FT and the fact that Lithuania has successfully prosecuted one FT case, the assessment team has no reason to believe that the mechanism in place to prosecute and convict persons for FT would not work effectively, should the need arise. The assessment team takes comfort from the fact that the prosecutors are aware of potential FT risks and specialised training is provided regularly on counter-terrorism and FT issues. At the same time, during the on-site visit, prosecutors underlined the need for more practical training, such as mock investigations and prosecutions, to be

held jointly with the Police. Moreover, as explained under core issue 9.2, there are some doubts about the ability of the authorities to effectively detect FT cases and the authorities have not carried out financial investigations in parallel with the terrorism cases that were investigated. This casts some doubts as to whether the low number of prosecutions and convictions is entirely in line with FT risks.

TF identification and investigation

205. The authorities indicated that there are mechanisms in place (discussed below) to identify FT cases through criminal intelligence investigations, on the basis of information received from foreign-counterparts, through formal and informal channels, on the basis of information from domestic authorities and STRs submitted by reporting entities. The Real IRA case appears to have been identified on the basis of a MLA request. The case identified in 2014 (referred to below) was brought to the attention of LEAs by the Committee on National Security and Defence of the Parliament of the Republic of Lithuania. It is unclear what the source of this information was.

206. One FT cases has been identified and investigated in the period under review. The case, which is still on-going, was opened in 2014. The assessment team posed a significant number of questions in order to determine whether the financing aspects of this case were properly investigated. However, the authorities were not willing to share substantial information, citing confidentiality, given that the case is still on-going.

Box 9.2

On 18 August 2014, a pre-trial investigation was initiated by the Vilnius Regional Prosecutor's Office pursuant to Art. 250-1 (1) (incitement of terrorist crimes), Art. 250-2 (1) (recruitment for terrorist activities) and 250-4 (1) (financing and sponsorship of terrorist activities) CC. The pre-trial investigation was commenced upon receiving a notice from the Committee on National Security and Defence of the Parliament of the Republic of Lithuania. It is unclear how the Committee identified this case.

In the course of the pre-trial investigation it was established that in 2014 a citizen of Lithuania attempted to recruit volunteers to go to a conflict zone to fight against the government of that country. In statements published on Facebook, he promoted support for separatist factions of that country. In addition, in 2014, the aforementioned person, together with others, registered at the Centre of Registers a public entity under the name "War and Peace". Having opened accounts at different banks in the name of the aforementioned entity, he raised funds for its benefit. The funds raised were used for purchasing medications and other items (which they named as donations), which then, were taken to the conflict zone with the aim of supporting possible terrorists. It is not clear what the amounts involved were and whether any STRs were received by the FIU.

In the course of the pre-trial investigation, cooperation was maintained with the following institutions: the Criminal Police Bureau, the State Tax Inspectorate, the District Court of Vilnius City, the Forensic Science Centre of Lithuania, and the State Medicines Control Agency and the Health Emergency Situations Centre under the Ministry of Health. Furthermore, requests for Mutual Legal Assistance were sent to two countries. Searches were carried out, information found on computers and telephones was examined, bank accounts held by the public entity "War and Peace" were frozen, witnesses were interviewed and other procedural actions were carried out.

Currently information provided by one country is being analysed and the decision to institute criminal proceedings is being considered.

State Security Department

207. The SSD is an intelligence body without investigation powers. It coordinates the fight against terrorism and FT within the country and demonstrated a higher level of understanding of FT risks

than the other authorities. The assessment team was informed that the SSD gathers and examines intelligence relating to FT on an on-going basis. In furtherance of this objective, it exchanges intelligence and information with other intelligence and security services of foreign countries and domestic authorities (no statistics were available). For instance, the SSD requests the FIU, the STI or the Customs Service to conduct certain actions (e.g. request information from foreign FIUs, provide bank account information, etc.) in order to determine whether the subject of the request is involved in FT activities.

208. The SSD has identified, and keeps under surveillance, some persons supporting Islamic fundamentalism in Lithuania. They are low profile and have been assessed to pose a very low threat. The SSD also focuses on the international threat, mainly in relation to the flow of foreigners through Lithuania, and on potential attempts to conduct terrorist attacks in Lithuania. Concerning the latter, the SSD actively monitors the territory to prevent terrorist attacks on Lithuanian soil. The SSD pays particular attention to potential "lone wolves" who could stage terrorist acts using their own resources.

209. Referring to returning FTFs, the SSD explained that as Lithuania is a border country of the EU, it is expected that some flow could go through Lithuania, through Belarus, Lithuania, Poland and Western Europe. So far, the SSD has not identified any transit of FTFs. The SSD collects intelligence and makes consultations with migration services when foreigners enter Lithuania from countries posing a high risk of terrorism. Applications for temporary permits or visas with respect to certain nationals are only issued upon consultation with the SSD following checks in relation to the applicant.

The FIU

210. As stated under IO 6, the FIU is responsible for analysing FT-related STRs. The FIU advised there have been some cases (although it is not clear how many) where a reporting entity identified possible terrorism suspicions or matches with persons or entities designated by the UN in TFS lists. Following analysis by the FIU, 18 reports were disseminated to the SSD for further intelligence actions. During the analysis, all bank documents and transfers of funds were requested and analysed in detail. The SSD found no need to refer the cases to LEAs for further investigation as no indication of FT was identified. As stated under IO 6, while banks are very much aware of the risks associated with FT, in discussions with certain representatives of the MVTS sector onsite, the assessment team came across cases which, on the face of it, would have warranted the submission of an STR for suspicions of FT. This could constitute a gap in the identification of FT cases in Lithuania. As explained in more detail under IO 10, after a review of the non-profit sector conducted by the FIU some cases were disseminated to the SSD. According to information provided on the result of the analysis of the a.m. reports no investigations were launched as the suspicions were not confirmed.

Criminal Police Bureau

211. The Lithuanian Criminal Police Bureau has a specialised unit which is trained on the investigation of FT and terrorism crimes. Ten units of the Police have the competence to conduct investigations into terrorism and FT as part of their activities.

212. In 2011-2017, 7 terrorism-related cases were identified and investigated by the Criminal Police. They were related to incitement to commit terrorist crimes, one to a terrorist act that caused damage to police cars and caused a loss and one relating to mercury found in a private residence. The analysis shows that the duration of investigations related to terrorism varies from 1 to 4 years and is longer in some cases. The Police did not look into the financial aspects of these cases. No financial

investigations were carried out, which is perhaps not surprising considering that the PG's Recommendations on financial investigations does not explicitly refer to terrorism and FT. The "historical" FT case shows that potential terrorists may seek to purchase weapons in Lithuania and seek the assistance of criminal groups in Lithuania for that purpose. Therefore, financial investigations conducted in parallel with investigations into predicate offences, such as smuggling, illicit weapon trading or organised crime groups may increase the capacities of authorities to identify not only ML but also FT.

213. A positive aspect of the system is that the Criminal Police Bureau, as a practice, when conducting criminal intelligence investigations in relation to certain offences, such as firearms trafficking, have started considering the possibility of the case being related to terrorism and FT. They have started looking at money flows, transferred for instance through money remittances, etc.

214. The Criminal Police holds training events on counter-terrorism, which, according to authorities, to some extent covers FT issues. The Lithuanian Criminal Police Bureau has organised and conducted the following trainings: April 2018 - Inspection of Explosives (together with the Forensic Research Centre); March 2018 - Terrorism, Internet propaganda and Radicalisation; March 2017 - Fundamentals and peculiarities of the fight against terrorism; and 2016 - Hatred crimes, Explosions.

215. In addition, the Criminal Police uses different channels for information exchange: Interpol, Europol, SIRENE, Prum. On 1 April 2015, access to Europol's Secure Information Exchange Network Application (SIENA) was granted to Unit 3 of Serious and Organised Crime Investigation Board 2 of LCPB (hereinafter referred to as LCPB CTU), which conducts criminal intelligence and criminal investigations in the field of terrorism and related criminal offences. In 2015, 433 messages were received and 117 messages were sent via SIENA; in 2016, 800 messages were received and 433 messages were sent via SIENA; and in 2017, 844 messages were received and 330 messages were sent via SIENA.

216. In February 2016, LCPB CTU joined the secure CT SIENA platform, which is only accessible to EU member states' counter terrorism units (the platform was designed as a point-to-point system without the involvement of ENU or Europol). On this platform, LCPB CTU received 384 messages and sent 93 in 2016; in 2017, 794 messages were received and 275 messages were sent.

217. The LCPB CTU is also a member of informal international networks of responsible counter terrorism experts (PWGT – Police Working group on Terrorism), which was established to allow counter terrorism units to conduct direct peer-to-peer exchange of sensitive information and intelligence on terrorist organisations/groups or persons and offences related to terrorism via the special SIENA system, which is accredited up to the SECRET level of confidentiality. In 2016, LCPB CTU received 180 and sent 139 messages; and in 2017, 80 messages were received and 59 were sent, as the system was stopped for 6 months period due to technical updates.

218. The exchanges generally involve: criminal intelligence, information about on-going investigations, various requests and reports, identity checks, invitations to meetings. Not all the messages referred to in the preceding paragraphs related to FT. Based on these exchanges, no FT crimes with links to Lithuania were identified.

The Customs Service

219. The Real IRA case, as well as ML-related cases, show that one of the possible ways to transfer assets for criminal purposes is through smuggling of cash over the borders. As stated elsewhere in the report, there is a high circulation of cash in Lithuania and the volume of cash transported in and

out of the country is significant. Despite of these risks, the Customs Service does not yet have the specific power to stop and restrain currency at the borders in order to ascertain whether evidence of FT may be found. This was confirmed by authorities met on-site. This raises some doubts about the ability of the Lithuanian authorities to identify and initiate FT enquiries at the borders. A number of case examples on predicate offences provided during the on-site visit show the widespread use of smuggled cash. In several cases, searches of suspects resulted in the detection of large amount of cash smuggled through the borders.

TF investigation integrated with -and supportive of- national strategies

220. On 7 May 2015, the Seimas of the Republic of Lithuania adopted the Public Security Development Programme for 2015-2025, whose aim is to ensure that Lithuania becomes a more secure state capable of effectively protecting fundamental human rights and freedoms and public security. The third goal of the programme relates to terrorism and FT. With a view to implementing this goal, the SSD established a working group which is aimed at dealing with issues related to the fight against terrorism and FT. The following institutions are involved in the activities of this group: the SSD, the Ministry of Interior, the Police, the FCIS, the VIP Protection Department, the State Border Guard Service, the PGO, the Ministry of Foreign Affairs, the Ministry of Justice, the Ministry of Culture, the Ministry of Social Security and Labour, the Ministry of Health and the Joint Staff of the Armed Forces of Lithuania. In October 2016, the first meeting of the CT working group took place. The members discussed and approved an action plan aimed at implementing the tasks of the Public Security Development Program (2015-2025). The assessment team has not received any detailed information on the actual and effective implementation of this action plan. It is not clear that this goal has found its way into the operational policies of either the Prosecution Service or LEAs and therefore no conclusion can be made as to whether the investigation of FT is integrated with, and used to support, national counter terrorism strategies and investigations.

Effectiveness, proportionality and dissuasiveness of sanctions

221. The sanctions provided in the CC for FT offences appear to be proportionate and dissuasive. During the period under evaluation, only one court decision was delivered in 2013, after the new provisions of the CC (new Article 250^4(1)) came into force. As a result, M.C. (case 1) was convicted for the disposal of firearms, ammunition, explosives, attempt to smuggling those items and FT (Article 250^4(1)). The most severe punishment was applied for FT. M.C. received the final consolidated sentence of imprisonment for 5 years, 8 months and 11 days. In addition, the instrument of the crime was confiscated, i.e. EUR 17,250.

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

222. The authorities have never applied alternative measures in lieu of proceeding with FT charges.

Conclusion

223. **Overall, Lithuania has achieved a moderate level of effectiveness for IO 9.**

Immediate Outcome 10 (TF preventive measures and financial sanctions)

Implementation of targeted financial sanctions for TF without delay

224. As a member of the EU, Lithuania relies on the EU framework for the implementation of TFS. The EU framework does not ensure that TFS are implemented 'without delay', since there is a delay between the designation decision taken by the UNSC and its transposition into the EU framework. The delay is caused by the application of a due diligence process in light of case law of the European Court of Justice leading to the adoption of a legally binding act to be published in the EU Official Journal. This is a serious impediment to Lithuania's effectiveness in preventing terrorists from raising, moving and using funds. The authorities suggested that the effective implementation of FT-related TFS while awaiting EU transposition could be ensured through freezing by the FIU in consultation with the MFA. However, since no such cases have arisen, it is unclear whether the process would be effective.

225. Lithuania does not have any cases to demonstrate implementation of TFS pursuant to UNSCRs 1267 and 1373, neither has it designated persons or entities that meet the designation criteria under the said Resolutions. While as noted under IO 9, the SSD monitors the territory of Lithuania to identify and prevent terrorism and FT, there is no mechanism aimed at identifying targets for designations and no proposal for designation had been made at the time of the on-site visit. The Lithuanian authorities also suggested that any state institution having information on potential targets would contact the MFA, which heads an *ad hoc* interagency committee comprising the SSD, the FCIS (including the FIU), the Criminal Police Bureau, the General Prosecutor Service, and the Ministry of Interior (MoI). The committee would take the final decision on whether a designation is to be proposed to the 1267/1989 or 1988 Committees. However, there appear to be no internal regulations within the MFA which specifically regulate the committee's functions and procedures in relation to proposals for designation.

226. The MFA is the authority responsible for co-ordinating the implementation of international sanctions in Lithuania. It provides information to natural and legal persons on the issues relating to the implementation of TFS. In practice, the MFA facilitates communication, discussion and the exchange of information between the relevant state authorities with respect to all sanctions regimes, including sanctions relating to terrorist financing and proliferation, arising at domestic, EU and international levels. This was also confirmed, while on-site, by the FCIS, the SSD, LEAs and other supervisory authorities. A sample of relevant electronic correspondence was provided to the assessment team while on-site.

227. All changes to the Consolidated United Nations Security Council Sanctions List are published in the Official Journal of the EU and the EU portal RSS. Following an update, the MFA receives a notification through the information system of Lithuania's membership in the EU – LINESIS. The MFA immediately sends a letter to all state supervisory authorities informing them of any changes. The updated list is also published on the MFA and FIU portals, which are accessible to all reporting entities. The FIU periodically informs reporting entities through letters reminding them to follow-up on the changes to the UN and EU sanctions lists. It is a prima facie obligation of the private sector to check both the UN and the EU designation lists. In practice, most financial institutions (FIs) subscribe to the EU RSS feeds to keep up to date with all new designations.

228. Both the FIU and the MFA have adopted a targeted approach in assisting banking institutions in their compliance with their FT-related TFS obligations. AML/CFT onsite inspections and training

activities by the FCIS, the BoL and the GCA include a FT-related TFS component. They consider that FIs have a good level of understanding of FT. During the inspections, some reporting entities were found not to be aware of the TFS regime. Although the FCIS has sanctioning powers in place, no sanctions or penalties have been imposed for breaches in this area. Instead, the authorities have addressed recommendations for remedial action. The authorities confirmed that all FIs and DNFBPs which were subject to this process took all the necessary measures to remedy the identified gaps. This was confirmed during follow-up inspections. Other supervisors exhibited limited understanding of risks entailed by sanctions evasion.

229. FIs, in particular the banking sector, have a good understanding of their freezing and reporting obligations. All banks have developed their own automated screening systems to check clients and beneficial owners of customers against sanctions lists. However, the awareness of the FT-related TFS obligations of the DNFBP sector is not as evident. Many rely on open source research to ensure that their business would not service designated individuals or entities, while some appeared to be completely unaware of their obligations. The authorities have indicated that the risk of FT in Lithuania appears to be low and have therefore supervised and monitored DNFBPs in relation to TFS on a level commensurate to their risk.

230. Guidance has been provided to REs on FT-related TFS. In particular, the FIU Instructions on Sanctions provide detailed guidance to REs on how to freeze assets of designated persons, while clarifying the designee's rights, duties, and the application of exemptions from sanctions. Information about de-listing, unfreezing and appealing procedures is also made available, while clarity is provided in relation to the application mechanism for TFS measures to "EU internals". The FIU, the BOL and other supervisors make TFS information available on their websites, respond telephonically to queries and undertake outreach via annual trainings and workshops. However, the overall communication approach adopted by the authorities is not yet sufficiently targeted. The supervisory authorities very often engage in TFS-related communication with REs, but this is mostly out of the latter's initiative. Also, training tends to be general in nature and only a small part is dedicated to TFS.

231. Lithuania implements UNSCR 1373 via the EU legal framework under the European Council Common Position (CP) 2001/931/CFSP and the EC Regulation 2580/2001. There are no formal procedures in place with regard to direct foreign requests to take freezing action pursuant to UNSCR 1373. Such requests are received indirectly through the regular EU channels of communication. Lithuania has never been requested by another country to take freezing actions pursuant to the UNSCR 1373.

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

232. Lithuania's non-profit organisations (NPOs) sector is composed of approximately 31,508 entities (table 20). The main legal forms in which NPOs operate in Lithuania are associations, public institutes and charity and sponsorship foundations. In 2017, the FIU undertook a FT review of the NPO sector, including the identification of the subset of organisations that fall within the FATF definition and those NPOs that are more likely to be at risk of FT. The review was based on STRs in relation to NPOs, which had cashed out more than EUR 80,000. Information on 75 NPOs which fulfilled the requirement were provided by the Lithuanian banking sector. The review did not reveal any indications of misuse of the NPO sector for FT purposes. These findings were in line with the 2015 NRA, which concluded that the FT risk of the NPO sector is of medium priority. As a result of the 2017 Strategic Analysis, the SSD received information in relation to the financial activity of 18

NPOs, while relevant information on 38 NPOs, which cashed out EUR 9,633,200 in total, were communicated to the FCIS.

233. Information on NPOs as required by the civil code is kept in the Register of Legal Entities (RLE), which is one of the five state registers of the Centre of Registers. The data of the RLE and all other information submitted to it are publicly available (see C.8.3)[62].

Table 20: Number of NPOs registered in the RLE

Registrar (branch of the Centre of Registers)	Association	Charity and Sponsorship Foundations	Public Institutes
Alytus	900	22	327
Kaunas	3502	288	1918
Klaipeda	1966	159	885
Marijampole	946	30	194
Panevezys	1461	53	366
Šiauliai	1883	106	404
Taurage	658	13	106
Telšiai	782	24	211
Utena	1112	39	260
Vilnius	5918	919	6056
Total	19 128	1653	1027

234. Although there is no historical precedent of NPOs being abused for FT in Lithuania, the NRA indicates that the FT risk of the NPO sector is of medium priority. The authorities explained that according to the scoring system of risk (likelihood, impact, vulnerability) adopted for the NRA process, the impact of the potential abuse of NPOs for FT would be significant (scoring 4 out of five), negatively impacting the total score. No NPOs were involved in the development of the NRA. Instead, information from the STI and FCIS from past inspections were used. Both the NRA and the authorities suggest that the NPO sector represents a high risk for tax evasion.

235. Lithuania has established a legal framework for interagency co-operation, co-ordination and information sharing among all relevant authorities (see C.8.5). The STI conducts oversight of NPOs from a tax compliance perspective. This oversight covers only general tax reporting obligations. If a NPO tax investigation or inspection reveals a ML/FT positive, the STI would transfer the case to the FIU. Reciprocal procedures are in place. In 2017, the FIU provided information to the STI on three NPOs suspected of tax violations and on criminal risks. Respective on-site inspections followed. In order to increase the efficiency of this process, the FIU amended the 2011 List of Criteria for determining the signs of possible ML/FT in the activities of NPOs (as amended by the FCIS Order No V-76, 10 April 2017). However, these criteria are only an addition to the focus of the STI supervision activities, which remains targeted on tax evasion issues.

236. The SSD considers that the risk of the NPOs abuse for FT is present in Lithuania, but it has not been materialised. Under its capacity to seek and collect FT-related information in Lithuania the SSD can obtain information on the activity, the size and the features of NPOs in a timely manner. The SSD shares all terrorism or FT – related information in relation to NPOs with all national authorities and

[62] http://www.registrucentras.lt/jar/p_en/

LEAs, in order to prevent the abuse of the sector. Currently, the SSD monitors closely approximately 30 religious NPOs, which fall under the FATF definition. However, the authorities did not provide further information on the identification criteria of such process.

237. No formal guidance, outreach or training on FT risks to NPOs or donor communities by the authorities has been carried out during the period under review. All NPOs met on-site were unaware of their obligations and the possible abuse for illicit activities including FT.

Deprivation of TF assets and instrumentalities

238. There has been no detection of any designated persons or entities holding accounts or assets in Lithuania under the TFS regime for FT. Therefore, no freezing of assets and instrumentalities of terrorists, terrorist organisations or terrorist financiers has been applied. It is the opinion of both the Lithuanian authorities and the REs, met on-site, that if assets or funds are located, these would be automatically frozen. The FIs met on-site, including all banks, also confirmed that upon a freezing action taken under the FT-related TFS regime, they would report the amount frozen to the FIU. In fact, banks had some cases of potential matches and that they notified to the FIU to be certain that they were false positives. Following analysis by the FIU, reports were disseminated to the SSD for further intelligence actions, although investigations were launched on the basis of these disseminations as the suspicions were not confirmed. This certainly adds to the effectiveness of the FT-related TFS regime of Lithuania. In the one FT conviction, which was achieved in 2017, the Court ordered the confiscation of the instrument of the crime i.e. EUR 17,250.

Consistency of measures with overall TF risk profile

239. The measures undertaken by the Lithuanian authorities are consistent with the country's overall FT risk profile. Relevant risk and threat assessments (2015 NRA and 2017 Strategic Analysis) and discussions with the FIU, the STI, the SSD and LEAs confirm this conclusion.

240. However, given the large size of the NPO sector and the geostrategic position of Lithuania, the outreach conducted is very poor. This is partly mitigated by the overall approach of most FIs in Lithuania, primarily banks, which pay close attention to national and international sanctions lists. In the same line, the representatives of financial technologies (Fintech) sector met on-site appear to be aware of their obligations stemming from the sanction regimes.

241. The Lithuanian authorities have adopted a number of action plans (e.g. NRA Action Plan) which set forth a number of priority actions in order to mitigate FT risks and improve the effectiveness of the system. In particular, with regard to NPOs the NRA Action Plan stipulates that i) the SSD should prepare an annual review of possible NPOs use for FT purposes; ii) the FCIS should update its List of Criteria; and iii) examine possible uses of NPOs for the FT purposes and provide identification criteria of such actions to NPOs themselves. However, most of these actions are underway.

Conclusion

242. **Lithuania has achieved a Moderate level of effectiveness for IO.10.**

Immediate Outcome 11 (PF financial sanctions)

Implementation of targeted financial sanctions related to proliferation financing without delay

243. Lithuania is neither a major weapons manufacturing country nor an international trade centre or a large market for proliferation goods. However, import and export statistics maintained by Customs Department indicate that exports to Iran had a value of EUR 239,095,300 in 2014 falling to EUR 7,106,700 in 2017, while imports from Iran totalled EUR 3,105,400 in 2014 and were EUR 3,987,300 in 2017. The trade with Iran relates to agricultural products, nuclear-related products[63] and plastics. Financial and trade flows with the Democratic People's Republic of Korea (DPRK) appear to be negligible.

244. The implementation of TFS for proliferation financing (PF) in Lithuania is based on the EU's legal framework set out in UN Security Council Resolution 1718 (DPRK) (Council Regulation No.329/2007, as amended, and Council Decisions 2013/183/CFSP) and Security Council Resolution 1737 (Iran) (Council Regulation No.267/2012 as amended and Council Decision 2010/413) respectively. Council Regulation (EU) 2015/1861 has introduced changes to take account of the Joint Comprehensive Plan of Action. As an EU member state, Lithuania is negatively impacted by the technical problems in the length of time between the designation of persons or entities by the UNSCRs and their transposition into the EU legal framework. Lithuania implements without delay the TFS defined in the UNSCRs relating to combatting PF with regard to Iran, but it does not do so with regard to DPRK. In particular, since March 2012 there have been only two occasions where the UN added designations to the list related to Iran (two entities and one individual on 19 April 2012, and two entities on 20 December 2012). In both cases, the designees were already listed in the EU framework (Regulation 1245/2011 of 1 December 2011, and Regulation 54/2012 of 23 January 2012), and subsequently incorporated into Annex IX of Regulation 267/2012.

245. The Lithuanian authorities do not contest the delays caused by the transposition system in place, although they argue that in practice, the risks are to a certain extent mitigated, as the EU applies sanctions to a larger number of entities that are not designated by the UN. In addition, they put forward the view that in practice service providers implement the UN TFS related to PF immediately as designations are made, before EU transposition. This was confirmed by most of the reporting entities met on-site.

246. The dissemination of TFS lists and outreach to the economic operators and export manufacturing sector of sensitive controlled goods and technologies as well as dual-use goods is carried out by the Investment and Export Division of the MoE (hereinafter "the Division"). The Division is responsible for the implementation of the EU export control regime as well as the EU's 'prior authorisation' process for transactions with Iranian entities under the Iran Sanction's regime and DPRK.

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

247. No cases of PF have been identified in the country and as a result no assets or funds associated with PF-related TFS have been frozen. No STRs were filed in relation to proliferation or PF, although there is no requirement to do so. There have been no investigations and prosecutions on PF, including in relation to border control. The authorities referred to several suspicions related to exports of aluminium powder and helicopter parts but none were confirmed as PF positive.

[63] Lithuania exports nuclear reactors, boilers, machinery, mechanical appliances and parts thereof to Iran

248. Banks implement PF-related TFS thoroughly. It is a prima facie obligation of all FIs to check the Although there have been no funds frozen in relation to trade with Iran and DPRK during the review period, assets have been frozen with regard to non-PF related sanctions. The Lithuanian authorities suggested that following the imposition of sanctions to an entity, the FIs in Lithuania immediately stop any transaction with it, even if this relates to non-listed goods. This has been confirmed during the interviews held on-site with the banking sector.

249. There is no national mechanism for coordination and implementation of policies and strategies to counter PF in Lithuania. As regards the administration of the implementation of international sanctions, the MFA has been assigned to co-ordinate the implementation of international sanctions and specified exemptions (Art. 11 of the Law on Sanctions). A weekly coordination meeting on policy issues takes place at the Cabinet of Ministers of Lithuania, which has in the past discussed PF-related matters. Nonetheless, the agenda of these meetings only occasionally include PF-related issues. Also, the Crisis Management Interagency body, as a permanent state body, assembles for urgent issues.

250. According to the government resolution (1679/2004) on sanctions the FCIS is responsible for the control and, on a regular basis, verification and collection of data on the implementation of financial sanctions.

251. The MoE is the licencing authority for import, transit and export of controlled goods. It monitors all activities in the field of export, import, transit and brokering of dual use goods and technologies as well as military equipment. Before issuing a licence the MoE carries out a control in order to verify whether natural and legal persons, branches of foreign legal entities, other organisations or intermediaries who export, import, or transit strategic and dual-use goods comply with the requirements of EU, international treaties and the legal acts of the Republic of Lithuania regulating the control of strategic and dual-use goods. Such a control is also carried out in order to determine whether the end-user has the right to dispose of and protect the goods, taking into account the purpose of the use of the goods, the adherence to prohibitions, restrictions and other requirements. The MoE provided information that continuous controls are carried out to licensed entities, while as a result of such controls licensed entities' activities may be suspended.

252. The authorities informed the assessment team that since 2016 approximately 300 requests for further information on the export of dual-use and strategic goods to Iran have been submitted, but none resulted into a request for authorisation. The Lithuanian authorities also informed the assessment team that since 2014 there have been two export authorisation requests which were denied in relation to the sale of military equipment to a company in the UAE. Although, the UAE is not subject of PF-related TFS, the MFA provided information on the risk of re-exporting the equipment to a third country, resulting in the rejection of the export requests.

253. The Customs Department is responsible for the control of strategic and dual-use goods. Its control system is based on a customs' declaration system. The Customs Department applies risk controls including for dual use goods (See Box 11.1). It carries out risk analysis and audit-based controls, along with randomly selected declarations. Being a member of the EU, Lithuania applies all European customs requirements. It requires all economic operators to provide pre-arrival and pre-departure information in relation to all the goods brought into or out of the territory. Pre-arrival and pre-departure information is submitted electronically via a new online system (Computerised Transit System). A strategy for the implementation of the common EU trade policy and security of the whole trade supply chain has been put in place by the Customs Department for the period 2016-2020.

Box 11.1

Prevention of dual use goods smuggling

Case 1

In 2016 the Vilnius regional court in an administrative case under the Ref. No. A2.11-11823-929/2016, related to unlicensed export of "Hydrofluoric acid", imposed a fine of EUR 800 to a Lithuanian exporter. The case was identified during risk profile validity controls in the national electronic Risk Management and Control system aimed at establishing the customs controls on export declarations in case when chemical substance under the Combined Nomenclature code (CN) subheading 2811 11 10). The identified declarations were lodged for the export procedure by one Lithuanian exporter to Belarus in 2016. In all these cases, the said substance, Hydrofluoric acid, was declared under CN heading 2811 11 10. No licence for the export of dual use was presented to Customs, but a virtual document under the code Y901. The latter raised suspicions that Art. 3 of Council Regulation No. 428/2009 (5 May 2009) on the export of dual – use goods had been violated. The Lithuanian authorities conducted an investigation in order to identify whether the exported Hydrofluoric acid is included in the Annex I of the Council Regulation (dual use goods exceptions). On the basis of the investigation result, an administrative case was initiated and the representative of the company was found guilty under the relevant articles of the Law on Administrative Proceedings and the Law on strategic goods.

Case 2

In 2011, while examining suspicious international trade transactions, the Customs came across to an export declaration submitted to the Lithuanian Customs Point by a consignor registered in another EU Member State. According to the single administrative document, the license request referred to 144 kg. of aluminium powder (high-risk explosive precursor chemical) of non-lamellar structure, with CN – 7603 10 00, to be exported to the Russian Federation. Due to the lack of certificates proving its chemical composition and the underlying risk, as aluminium powder id classified to be a dual – use good (Council Regulation No. 428/2009 of 5 May 2009), the Customs decided to refuse an export license.

Relevant information from both cases presented above were submitted to other EU member states.

254. On combating illicit trafficking in nuclear and other radioactive material, the Customs Department performs robust controls within the territory of Lithuania (both at land borders and at airport terminals) through the use of a mobile radiation detection system. The Customs Training Centre provides training in relation to this system. The authorities have the power to impose fines on those involved in the trafficking of nuclear and radioactive material. However, no fine has been imposed since the last breach, which dates back to 2009. The assessment team discussed the contents of an article which referred to a number of incidents related to the smuggling of nuclear material (see issue of increased focus). The authorities confirmed that no other incident of relevant nature had taken place since 2009 (prior to the review period) and they were confident to present a robust system set in place for the detection of nuclear and other radioactive material (see below).

Box 11.2

Nuclear and other radioactive material controls

Monitoring is performed by five Mobile detection teams. Each team consists of three customs officers. The customs officers inspect: radiation and documents, as well as customs declarations (particular attention is being paid to transported dual-use goods), vehicle marking, permits, licenses, goods.

When performing control of nuclear and other radioactive materials, the radiation detector has an active alarm which provides a signal on contaminated wood and wood panels, fertilizers, pottery (ceramics) products, mineral wool and glass fabrics.

On combating illicit trafficking in nuclear and other radioactive material, the Lithuanian Customs cooperates with the State Border Guard (especially in the area of officers' training), the Radiation Protection Centre (in the

area of information exchange), the VIP Protection Department (joint actions), and the Police Department (joint inspections on the road).

FIs and DNFPBs' understanding of and compliance with obligations

255. FIs, in particular the banking sector, are well-aware of their obligations on PF-related TFS. Banks apply a very strict approach to ensure compliance with sanctions obligations and are very wary of sanctions evasion consequences. The Lithuanian authorities provided information on 10 instances where banks refused payments which were not subject to international sanctions (e.g. banks flag transactions with regard to Iran). The FIs and DNFBPs rely mainly on controls implemented for CDD purposes, which are aimed at identifying beneficial ownership, despite the challenges on verification of identity of beneficial ownership of legal persons with foreign beneficial owners and complex ownership structures (See IO.4). Awareness of risks among DNFBPs is generally limited to awareness of sanctions lists and seemingly sporadic screening against them. This also reflects the fact that a few supervisors (the Chamber of Notaries, the Chamber of Auditors, the Lithuanian Assay Office, and the Bar Association) exhibited limited understanding of risks entailed by sanctions evasion. The representatives of financial technologies (Fintech) sector met on-site appear to be aware of their obligations stemming from the sanction regimes.

Competent authorities ensuring and monitoring compliance

256. The authorities have indicated that the PF risk in Lithuania is relatively low. The MFA disseminates UN sanctions lists to obliged entities by email, and posts links to both UN and EU sanctions lists on its website[64]. It also provides outreach and guidance according to the needs identified, although of a generic nature. In fact, the MFA has issued Instructions on Sanctions (see IO.10, R.6 and R.7). However, they do not mention explicitly proliferation or proliferation financing sanctions and therefore do not appear well suited to provide adequate guidance on PF. The MFA and the FIU regularly receive requests for assistance from the banking sector when it comes to transactions to Iran. The MoE regularly holds workshops for industry associations where it introduces updates concerning licencing requirements and sanctions lists.

257. The mechanism for ensuring compliance by REs with the requirements on PF is carried out by each supervisor pursuant to its respective regulations on the implementation of financial monitoring (see IO3). Most of the supervisory authorities met on-site include the verification of PF-related TFS obligation in their respective inspection procedures, although, it is unclear what level of priority is assigned to verifying PF-related obligations. During inspections the authorities identified breaches, as some FIs and DNFBPs were not aware of the TFS regime related to PF. No sanctions or penalties have been imposed. The authorities have indicated that recommendations have been made, which have all subsequently been remedied as confirmed through follow-up inspections.

258. The BoL apart from on-site inspections, in its annual questionnaire sent to the supervised financial market participants requires all FI's to describe their internal procedures used to determine whether a client and/or beneficiary is subject to UN or EU restrictive measures. Information in relation to the deployment of special automated systems for such a purpose, types of data systems etc. is also required. In addition the BoL has issued guidelines/instructions for the securities and

64 https://www.urm.lt/default/en/foreign-policy/lithuania-in-the-region-and-the-world/lithuanias-security-policy/sanctions

insurance sector which establish the procedure for implementation of the legal requirements available on the implementation of international sanctions.

Conclusion

259. **Lithuania has achieved a moderate level of effectiveness for IO.11.**

CHAPTER 5. PREVENTIVE MEASURES

Key Findings and Recommended Actions

Key Findings

1. Banks have a good level of understanding of ML/TF risks and are aware of their AML/CFT obligations. Non-bank FIs generally have a satisfactory understanding of ML/TF risks but weaknesses were identified in relation to MVTS and currency exchange offices. Some of these FIs did not demonstrate an understanding of how their sectors could be used for TF.

2. Understanding of ML/TF risks among the DNFBP sector is not sufficient. Casinos, notaries, lawyers and auditors were aware of their AML/CFT obligations while other DNFBPs such as real estate agents, tax advisors and traders over EUR 10,000 in cash had a very limited knowledge of their obligations.

3. The application of CDD measures (including enhanced CDD) by FIs is strong, particularly by banks, although verification of BO information in cases where there are complex structures or where legal persons are owned by foreign legal persons poses a challenge. This is mitigated by the fact that such customers are rare. The application of adequate CDD measures by some DNFBPs (particularly real estate agents and dealers) is not very developed, with very limited understanding of the minimum requirements set by the law.

4. While the private sector generally understands the procedures for reporting to the FIU (except currency exchange offices and most of the traders over EUR 10,000), the evaluation team expected to see more STR output from MVTS, currency exchange offices, real estate agents, notaries and lawyers. In fact, the vast majority of STRs are made by banks. Deficiencies have also been noted where in case of suspicious element, professionals refused to establish the business relationship without submitting a STR to the FIU.

5. Banks have put in place strong internal controls, which include various lines of defence; internal audit, automatic systems for transaction monitoring, periodic reporting to the management, access to commercial databases and appropriate human resources. Non-bank FIs have varying levels of internal controls in place, although it appeared that they were adequate in view of the risk and business conducted. Casinos appeared to have adequate internal policies and internal control procedures. Other DNFBPs (such as notaries, lawyers, real estate agents) indicated that they do not have AML/CFT compliance structures in place as the majority of them are sole practitioners.

6. Most non-bank FIs and DNFBPs have indicated that sector-specific guidance and training is needed from their supervisors.

Recommended Actions

1. Lithuania should take appropriate measures to raise awareness of all FIs and DNFBPs of ML/FT risks, particularly the risks associated with high level cash turnover, and ensure that EDD measures are applied consistently, especially in relation to cash transactions.

2. Lithuania should take into account the risks related to the use of cash in real estate transactions and consider implementing mitigating measures in order to reduce related risks (e.g. introduce a maximum threshold).

3. Authorities should ensure that non-bank FIs and DNFBPs conduct regular assessments of their ML/TF risks for customers, products and services. The risk assessments should be appropriate to the nature and size of the business and take into account the results of the NRA.

4. Supervisors and/or the FIU should broaden their training programmes for all types of REs (including REs operating in Lithuania licensed in another EU member state) to raise awareness of:

- the risks (including TF risks) identified in the NRA with a specific focus on distinct risks facing each sector and relevant mitigating measures to be taken,

- identification and verification of BO information,

- reporting obligations (including difference between CTRs and STRs) and criteria on suspicion specific to the sector.

5. Non-bank FIs and DNFBPs should develop and implement mechanisms that ensure more systematic monitoring of transactions with a view to identifying suspicions of ML/FT (e.g. by developing tools and knowledge of indicators specific to their sector in order to properly identify and disclose suspicious translations).

6. The authorities should promote a better understanding of ML/FT risks among DNFBPs and ensure that enhanced due diligence measures are applied in relation to high risk customers.

Immediate Outcome 4 (Preventive Measures)

260. Financial services in Lithuania are mainly provided by the banking sector composed of six banks (three of them hold the majority of the assets) and seven foreign EU bank branches. Compared with the banks' market share in the Lithuanian economy, other financial institutions, including the Fintech sector, account for only a marginal market share. Detailed information is provided in Chapter 1.

261. Financial services are provided largely to residents of the country. Only 2% out of the total number of bank customers were non-residents in 2017. The few non-resident customers, holding 2,3% of the total deposits in banks (461 million EUR) and 1,8% of the total loan portfolio (336 million EUR), are mainly natural persons (96% out of the non-resident customers) from neighbouring countries (top 3 countries Ukraine, Belarus and the Russian Federation),Lithuanians living abroad and few foreign businesses (3,056 non-resident legal persons out of 257,161 total legal persons of bank customers) which service customers in Lithuania. During the last few years, banks have reduced the provision of services to offshore companies and the majority of the banks refuse to enter into business relationships with offshore companies when there is no economic link with Lithuania. Regarding high risk customers (PEPs[65], persons residing in high risk countries, customers qualified as

[65] 0,27% of the total number of customers in banks in 2017 were PEPs. Assets held by resident PEPs: 41 million EUR; Assets held by non-resident PEPs: 1,2 million EUR.

high risk on the basis of internal risk management systems), the number was about 1.6% of the total number of customers in banks in 2017.

262. All types of DNFBPs are present in Lithuania except trustees. The sector has no specific features and the services provided by operators are of a traditional nature. 19 casinos are present in Lithuania and 6 online casinos. It is also to be noted that the evaluation team did not meet any company service providers as there were no registration requirements for the sector at the time of the on-site visit (see IO3).

Understanding of ML/TF risks and AML/CTF obligations

Banks

263. The Lithuanian financial system is dominated by banks offering basic retail banking services, leasing and insurance services. There is some concentration in the banking sector, with three banks dominating and accounting for almost three quarters of the sector in terms of assets; these three banks are foreign-owned

264. In general, the banks demonstrated a good level of understanding of ML risks and have implemented tools which allow them to mitigate those risks. All of the banks interviewed understand their obligations under the AML/CFT. Banks carry out risk assessments which include different types of risks, such as customer risk, product or service risk, operational risk, country-based risk and/or geographical area risk. The risk assessments generally take into account the results of the European Commission's assessment, as well as the Lithuanian NRA. Risk assessments conducted by banks, in particular those that are part of a group, are very comprehensive and take account of the specific risks that they face and the group's assessment system. Most of the banks demonstrated that their assessments are updated at least annually. However, the assessment team retains some reservations with respect to risk understanding by banks, given that the quality of STRs by banks is still not up to a satisfactory level (as indicated both under core issue 6.2 and core issue 4.5).

265. Most of the interviewed banks have a satisfactory understanding of risks identified in the NRA while their involvement in the process mainly constituted completion of the questionnaires. Generally, banks agreed with the risks identified in the NRA, such as the cash-based economy and high level of shadow economy to be the main threats in the country and have preventive measures in place. Banks categorize cash transactions as high risk and apply enhanced measures in relation to them mostly when the transaction exceeds EUR 15,000 (in some cases EDD is applied even if the transaction is less than EUR 15,000) by requiring more substantiating documents to approve the origin of funds. Banks advised that cash is mostly used in the real estate and construction sector. There is also a significant use of cash by car dealers in relation to cars purchased and sold outside Lithuania (the city of Kaunas hosts an important used car market and import/export hub[66]) and to a lesser extent by tourists from non-EU neighbouring countries preferring cash payments for their expenditure.

266. Interviewed banks risk rate their customers prior to establishing business relationship, generally using low, medium or high ratings. Most clients are medium risk. The main criteria for high risk customers generally include

[66] Banks indicated that used cars are mainly bought in western European countries and sold to central Asian countries like Kyrgyzstan. The car market is open seven days a week, covers an area of 200,000 square meters and exhibits around 6,000 cars a day (doubled on Saturdays).

- domestic and foreign PEPs;
- non-resident legal persons;
- cash intensive businesses;
- persons from countries, which:
    a. do not apply the FATF standards;
    b. are subject to sanctions, embargos or similar measures;
    c. have a high level of corruption.

267. In some cases, banks categorise all customers from outside the EU as high risk.

268. The number of high risk customers has recently increased due to the extended definition of PEPs, which since 2017 has included persons with prominent public functions in Lithuania.

269. Very few banks advised that they have customers that are foreign trusts and confirmed that they do not have any customers who hold bearer shares.

270. According to data provided by banks, the number of customers that are companies from offshore jurisdictions has significantly reduced. Onboarding a non-resident legal entity customer is an exception. Some banks have advised that they have opened accounts for companies from offshore jurisdictions only in cases when they had some form of relation to a Lithuanian company or conducted activities in Lithuania.

271. Banks demonstrated a good understanding of the risks related to fictitious companies. There appear to be controls in place and adequate measures are undertaken to ensure that a company is not fictitious. These measures include crosschecks of documents, asking questions about the activity of the company, confirming the real address of the business location, organising interviews with customers, and analysing payments and sensitive activities. Banks see these controls and their focus on cash as addressing the risks of the shadow economy.

272. Understanding of FT risk by banks as well as related obligations is rather good. Banks share the view of the authorities by qualifying FT risk as low; banks' focus more on ML is not related to a misunderstanding of FT risk but linked to the results of the NRA and their own risk assessments.

Non-banks FIs

273. The understanding of ML/FT risks varies among non-bank FIs. Understanding of risks by the MVTS sector and currency exchange offices is lower than the other FIs. Most non-bank FIs also consider FT risk to be low but there is relatively insufficient understanding of the underlying reasons. Risk assessments conducted by some non-bank FIs are limited to the risk criteria set out by the law and they were unable to demonstrate which risks were pertinent to their activities. As for involvement in the NRA process, only life insurance undertakings, leasing companies and credit unions were involved in the process by filling in respective questionnaires.

274. The *securities sector* is very small in Lithuania and it provides services only to small and medium-sized companies and individuals. The sector does not deal with cash. Securities firms are more inclined to refuse the establishment of business relationships than other sectors when the ML/FT risks are not understood, as they do not have enough awareness of the measures to be taken in such cases. Representatives of the sector confirmed that they lack knowledge of sector-specific risks and that there is a need for further guidance or training for the sector.

275. *Asset management companies* demonstrated good understanding of ML/FT risks identified in the NRA, though not other risks specific to their sector. They believe that the NRA is more bank

oriented and does not specify risks in other sectors. Services provided by companies mostly relate to the government pension fund system and they do not provide management services for foreign funds. Most transactions do not involve funds which exceed EUR 2,000.

276. In the case of *life insurance companies,* they advised that they provide services only to Lithuanian residents and do not deal with cash transactions. Clients can terminate contracts within a maximum of 30 days without a fee. In such cases the funds are returned to the customer; beneficiaries of policies do not receive the funds. High risk customers mostly comprise domestic PEPs. It is believed that ML or FT risks in the life-insurance sector are very low. In general, firms understand their obligations.

277. The *MVTS sector* is essentially represented by large international money transfer companies which provide their services through their agents in Lithuania, i.e. by the Post of Lithuania and by certain banks. When offering money transfer services, the different agents apply the MVTS company's policies and use the dedicated equipment and tools (mainly money transfer and related IT systems) provided by the MVTS company. While money transfer agents have to identify customers and enter their data in the IT systems, the MVTS companies operate automatic screening of customers and monitoring of transactions. In this regard, the MVTS companies' understanding of ML/FT risks varies significantly. Some of them have a satisfactory level of risk assessment documentation, which are updated periodically, with monitoring systems in place with various scenarios; others could not demonstrate how their sector could be used for FT. All the representatives met mentioned that the main purpose for using their services is family support. Certain MVTS representatives were unaware of TFS obligations and the practical measures for their implementation[67].

278. The *Fintech sector* demonstrated a generally good understanding of ML/FT risks. All regulated Fintech entities (EMIs, crowd-funding platforms and P2P lending platforms) met on-site had conducted their own risk assessment before launching their products or services, although not entirely related to ML/FT risks and vulnerabilities. Most of these entities allow deposits only through bank accounts or credit cards and were aware of their obligations to apply AML/CFT measures.

279. All representatives of entities offering virtual currency exchange services met on-site confirmed that they apply AML/CFT measures. Despite of this, some entities demonstrated limited understanding of their ML/FT risks and the very factors dictating AML/CFT measures. Virtual currency exchanges allow deposits through a variety of means, such as bank accounts, credit cards, mobile balance, etc. All representatives met on-site consider that the ML/FT risk is low within their sector, as they adhere to the AML/CFT requirements applied to all FIs, although most of them are not so obliged by law. Virtual currency entities met on-site indicated that larger banks usually refuse to deal with them for reputational considerations. Only small banks and e-money institutions accept payment from cryptocurrency exchange providers.

280. *E-money institutions* represent a major part of the Fintech sector in Lithuania. 29 entities are licensed but only 10 of them carried out activities as at December 2017. According to the assessment conducted by the BoL in 2016, more than 2/3 of the evaluated institutions are to be regarded as exposed to low ML/FT risks. Further analysis showed that seven payment and e-money institutions, based on the nature of their activities, services and clients, are exposed to medium to high ML/FT

[67] Electronic money institutions and payment institutions whose registered office is in another European Union Member State providing services in the Republic of Lithuania through agents, natural or legal persons are regarded as the obliged entities under AML/CFT law since 13th July 2017 (when new AML/CFT law came into force)

risks and two payment and e-money institutions are exposed to high ML/FT risks. As opposed to banks, The number of customers has significantly increased in the e-money sector in 2018 as against 2017, including customers from high risk countries: i) the number of high-risk countries from which customers are is higher than for banks and ii) companies from offshore jurisdictions are also using the services offered by PIs and EMIs). This increase is believed by the sector representatives to be conditioned by the fact that the services they provide are cheaper than in banks.

281. *Currency exchange offices* have very limited understanding of ML/FT risks. They equate AML requirements to identification procedures. *Lending companies* have adequate understanding of their ML/FT risks and obligations. Usually, they provide services to domestic small-medium companies, and make onsite checks to mitigate the risk of false or falsified invoices. *Credit union* representatives confirmed that the risk is low in their sector as they have a good knowledge of their clients, who mostly apply for credit to buy a flat or to finance studies or goods; in addition, they have few transactions in cash.

DNFBPs

282. Understanding of ML/FT risks among the DNFBP sector is not sufficient, except for casinos. Some DNFBPs consider that risks are mitigated as transactions are conducted via banks. Almost all DNFBPs were certain that their exposure to ML/FT risk is low as they usually do not deal with high risk customers and the amounts included in the transactions are not high. They were not fluent in articulating risks associated with their sector. Mostly, they classify customers as high risk when they are PEPs and resident in high risk jurisdictions.

283. Some DNFBPs (e.g. real estate agents, lawyers) do not recognize fictitious companies to be common in Lithuania. Also, they do not believe that there is intensive use of cash in the real estate sector. Real estate agents and lawyers interviewed see risks with regard to the use of cryptocurrencies. DNFBPs which were aware of the NRA did not find it useful for their sector.

284. *Casinos* demonstrated a relatively good understanding of ML/FT obligations. They explained that their risk assessments are reviewed on an ongoing basis. However, this could not be confirmed as no supporting documentation was provided to the assessment team. Casinos only deal with cash and it is common for them to convert chips into cash. Customers can request the casino to transfer winnings to their bank accounts and some casinos stated they have performed such transactions.

285. *Notaries'* involvement is mandatory for real estate transactions. All notaries have a deposit account with banks and buyers use this account to make a payment. *Lawyers* met by the assessment team reported that they do not have pooled accounts in banks though they mentioned that it is not uncommon for other lawyers. According to the BoL, these accounts are not maintained on a non-disclosed basis. Notaries and lawyers demonstrated satisfactory knowledge of AML/CFT obligations. *Traders over EUR 10,000 in cash* do not understand their role in the AML/CFT system. *Auditors* interviewed were from auditing firms which are subsidiaries of the world's biggest auditing firms and one representative of Small and Medium-Sized Practices (audit firms), which provide a high level of professional activity, including in terms of the adequacy of compliance and internal control systems. *Real estate agents* and *accountants* demonstrated relatively low level of understanding of ML/FT risk and their obligations.

Application of risk mitigating measures

286. Mitigating measures taken by the private sector are risk-based, except for some DNFBPs (e.g. real estate agents, traders over EUR 10,000 in cash). Generally, customers are categorised as low, medium or high risk. Depending on the level of risk, simplified, standard or enhanced due diligence measures are applied. Most FIs and DNFBPs were aware of the additional measures required when a customer poses higher risk. However, the risk of some products does not seem to be duly considered (e.g. cryptocurrencies, pooled accounts by notaries and lawyers, etc.).

287. Adequate automatic screening controls and monitoring systems are always used by banks to mitigate the identified risks. Controls are reviewed periodically, at least once a year.

288. Almost all the representatives from the private sector mentioned that they refuse to conduct transactions or to establish business relationships when requested additional documents on the legal purpose of transactions, are not presented.

289. Cash transactions are categorized as high risk by banks and most non-bank FIs which deal with cash, and enhanced measures are taken in order to understand the origin of funds. When the required information is not provided, the transaction is not carried out. Currency exchange office representatives met onsite and some DNFBPs consider filing CTRs with the FIU to be sufficient. They do not appear to initiate further analysis for monitoring purposes in order to determine whether additionally, STRs should be filed with FIU.

290. Supervisory authorities and the FIU provide regular trainings and consultations for the private sector, with a particular focus on mitigating measures based on the level of risk. Banks appreciate the content and number of trainings provided. However, some FIs and DNFBPs pointed out that more sector-specific training on the control and the mitigation of risks is needed. The compliance unit (officers) of financial institutions and some DNFBPs organise internal trainings focussing on risk-mitigating measures.

Application of CDD and record keeping requirements

291. The private sector, with the exception of some DNFBPs (e.g. real estate agents, dealers in cash over EUR 10,000), have adequate identification and verification procedures in place. All banks reported that they would not make a transaction and/or establish a business relationship with a customer when they fail to collect the required information. The identification and verification procedures for customers that are natural persons are applied to directors and other legal representative of legal persons and BOs. Representatives of non-bank FIs as well as most of the DNFBPs met on-site reported a similar approach. The assessment team was not convinced that real estate agents and traders would refuse business in case they fail to collect the required information.

292. Casinos identify and register clients when they enter the premises of the casino, regardless of whether they intend to gamble. Currency exchange offices identify clients when the amount exceeds EUR 3,000. However, they do not have any mechanisms to identify cases when a person exchanges in several transactions which in total exceed EUR 3,000. In most cases, MVTS providers apply stricter requirements than those required by the standards and identify clients even though the transaction amount does not exceed EUR 600.

293. FIs and some DNFBPs verify BO information using Lithuanian registers and registers of other countries. One recurring difficulty that must be noted and which concerns both FIs and DNFBPs is the ability to verify legal persons' BO information in the case of complex structures or when the legal person is owned by a foreign legal person. In these latter cases, which are a minority, the verification

of BO information through the usual process of checking information contained in the Register of Legal Entities is more challenging and sometimes cannot be achieved. When they fail to verify the UBO, as is mostly the case with legal persons with a complex structure, they refuse to establish a business relationship. Most DNFBPs confirmed that they lack knowledge of how to verify the UBO. Some non-bank FIs (particularly the insurance sector) had difficulties in demonstrating their understanding of the concept of BO in cases where a natural person acts on behalf of another natural person. Nevertheless, it appears that FIs will not in all cases consider filing an STR with the FIU when they have a doubt about the real BO and refuse to establish a business relationship.

294. With regard the timing of verification of identity, the law allows for the establishment of business relationships when opening an account without verifying the customers' identity, if the risks are mitigated. However, delayed verification is not a common practice for the private sector.

295. When establishing non face-to-face business relationships banks undertake all of the measures stipulated by law, including identifying customers by video streaming. Some banks provide non face-to-face identification services only for Lithuanian residents. However, there are certain doubts about the adequacy of the non-face-to-face identification/verification processes of e-money institutions. In particular, it is not clear whether payments can be made into the customer's account from accounts held in the name of persons other than the customer before making use of the service.

296. Real estate agents and dealers in cash over EUR 10,000 demonstrated a low level of understanding of the minimum requirements set by the law. It was reported that real estate agents are not engaged in any financial transaction.

297. FIs very randomly (one interviewed bank, one e-money institution, and entities from the Fintech sector) make use of information on the customer or the beneficial owner from third parties when establishing the identity of the customer or the beneficial owner.

Record-keeping

298. Records on monetary transactions and business relationships, data on customer, beneficiary and beneficial owner are required to be kept for 8 years from the date of termination of transactions or business relationships. Business correspondence with the customer must be stored for 5 years. The private sector has a good understanding of record keeping requirements. In practice, they maintain documents for the period required by the law.

Application of EDD measures

PEPs

299. The legal framework covers both foreign and domestic PEPs. All FIs and most DNFBPs (except currency exchange offices) have a good understanding of enhanced measures in relation to PEPs, and they have adequate measures in place to determine whether the customer and the beneficial owner are PEPs. FIs indicated they receive approval from a senior manager before establishing or continuing business relationships with such customers. EDD is performed by applying additional measures in relation to PEPs to establish the source of wealth and funds connected with the business relationship or transaction.

300. Only a few of those interviewed (asset management companies and some banks) mentioned the Chief Official Ethics Commission (where data is available of the declarations of private interests of PEPs who have been entrusted with prominent public functions in Lithuania) as a source of

information on domestic PEPs. Declaration data is public. Most of those interviewed mentioned that they use the Dow Jones database to verify PEPs. They indicated that they have difficulties in practice as there are no sufficient and centralized databases for PEPs, including their family members or close associates. In addition to the verification of PEP status using well known commercial databases, there is a common practice among FIs to obtain a self-declaration by the customer as to whether he/she is considered as a PEP (the questions on the links with PEPs are usually included in KYC questionnaires that are required to be submitted during on-boarding process and regularly updated thereafter). Casinos and currency exchange offices have questionnaires on PEPs which are completed by the clients. Casinos perform open source checks to verify information on PEPs.

Correspondent Banking

301. There are a few banks providing correspondent banking services to respondent institutions which are generally EU banks belonging to their group. Only one bank licensed in Lithuania also provides correspondent banking services to non-EU banks, all of which are situated in Belarus. The BoL advised that the average flows of non-EU correspondent banking activities amounts to several thousand per year, although the exact figures could not be provided. In these cases, EDD is carried out, which include questionnaires with specific questions on control mechanisms, business nature, etc. and requiring senior management approval before the relationship is established. Correspondent relationships are subject to periodic reviews. Awareness of and compliance with regard to correspondent relationships appear to be in line with the required standards.

New Technologies

302. All FIs interviewed were aware of the requirement to assess the ML/FT risks related to the implementation of new services and products, and the use of new (developing) technologies in business. In practice, it is mainly banks and most of the Fintech sector which conduct such assessments, as the other FIs rarely deal with new technologies or launch new products.

Targeted Financial Sanctions

303. Banks and other FIs have a good level of awareness of UN and EU designations, and they have developed automatic systems to monitor customers against those lists. DNFBPs demonstrated limited understanding and implementation of these obligations, although it is unlikely that they are exposed to such risks. The Fintech sector has good awareness of TFS-related obligations. No assets or funds have been frozen. Contrary to the view of the supervisory authorities, non-bank FIs and DNFBPs reported to the assessment team that little training has been organised by the authorities on TFS.

Wire Transfer Rules

304. In Lithuania, money remittance services are provided through banks and the Post Office as agents of global MVTS providers (MoneyGram, Western Union, Unistream, Contact). Representatives of the sector appeared to be aware of the requirements of Recommendation 16. Banks advised that wire transfer information is automatically screened by the system. Checks are carried out periodically to ensure that wire transfers contain all required data. In cases of missing information, banks contact the originator's institution and request additional information, before proceeding with the transfer.

Higher-Risk Countries

305. Most private sector entities interviewed demonstrated satisfactory awareness of their obligation to assess geographical risk factors when identifying whether there is higher risk of ML/FT, the exceptions being a few DNFBPs (real estate agents, traders over EUR 10,000 in cash, accountants). The following are considered to pose a higher risk: countries identified by the FATF as non-compliant with the Standards; countries identified as having a significant level of corruption or other criminal activity, and countries subject to sanctions, embargos or similar measures issued by, for example, the European Union or the United Nations.

306. The list of higher risk countries is more extended in the case of banks to include offshore jurisdictions and countries identified as high risk by their parent (in cases where the bank is part of a group). Banks have automatic IT systems and tools to monitor incoming and outgoing transactions based on specific criteria incorporated within the system. However, some MVTS providers do not appear to take reasonable measures to monitor payments, for example, made to high risk countries.

307. Country risk is one of the most common factors used by the private sector to assess customer risk. EDD measures are taken in relation to such customers which focus on determining the purpose and nature of transfers, and the source of funds involved in the transfers.

308. Those interviewed reported to the assessment team that the FIU and supervisory authorities do not provide any lists of countries which are considered to pose a higher risk.

309. Some DNFBPs (real estate agents, traders over EUR 10,000 in cash, accountants) demonstrated poor understanding of higher risk countries and did not refer to the application of any EDD measures.

Reporting obligations and tipping off

310. Generally, the private sector (both FIs and DNFBPs) was found to be aware of its reporting obligations with the exception of currency exchange offices, which have difficulties in distinguishing STRs from CTRs, and one major MVTS provider operating in Lithuania licensed in another EU member state, which only submits STRs to the FIU on a voluntary basis. Most of the traders met on-site did not demonstrate any knowledge of reporting obligations.

311. Although it is very common to refuse the establishment of a business relationship or not to conduct a transaction in case of suspicion, the private sector does not always consider submitting STRs to the FIU. However, it is a common practice by FIs to maintain a "black list" of customers (amongst the reasons for a customer to appear on the list is non-cooperation and increased ML/TF risk identified during an unsuccessful on-boarding process).

312. The statistics on reporting are presented in Table 8 under IO 6. In view of the fact that banks hold a dominant share of the financial sector and that a significant volume of financial transactions are carried out by banks, it appears reasonable that a substantial majority of STRs are submitted by banks. The assessment team has concluded that the number of STRs submitted by banks has increased over the last 3 years due to the development of their internal control systems, including advanced IT tools. Some non-bank FIs met on-site have not identified any suspicious cases. In their view, the nature of their activities is not considered vulnerable to ML/FT. Most representatives from non-bank FIs explained that they lack the tools and knowledge of indicators specific to their sector in order to properly identify and disclose suspicious transactions. The authorities have not considered whether the reporting levels by the other REs e.g. currency exchange, insurance, securities, etc. are adequate.

313. With regard to the DNFBP sector, casinos demonstrated higher awareness of suspicious transaction indicators and frequently submitted STRs, which mostly related to cases when a client regularly exchanges chips into cash or cash into chips without gambling, or the exchanged amount did not exceed EUR 15,000. This seems to be consistent with the risks emanating from the sector. The low level of reporting by some DNFBPs, in particular lawyers, notaries and real estate agents, appears to be inconsistent with the risks identified in these sectors.

Tipping-off

314. Representatives from the private sector, in particular those that submit STRs, were aware of the prohibition on tipping off. There have been no cases involving tipping off. Training conducted internally by FIs and most DNFBPs appears to include matters related to tipping off.

Internal controls and legal/regulatory requirements impending implementation

315. Most of the private sector entities have compliance officers with sufficient seniority and knowledge of the institution's ML/FT risk exposure. They are responsible for taking decisions affecting the institution's risk exposure.

316. Banks implement group-wide policies and procedures for the prevention of ML/FT in compliance with the national legislation. At least one member of the board is responsible for the implementation of AML/CFT measures. All banks have appropriate control systems in place to mitigate ML/FT risks. Those controls include various lines of defence; internal audit, automatic systems for transaction monitoring, periodic reporting to the management, access to commercial databases and appropriate human resources. They seemed to be sufficiently staffed. Periodic AML/CFT training is organised for staff. Specific training is organised for new staff and for management. Internal audit programmes always cover AML/CFT. The breaches identified through internal audit generally relate to KYC procedures.

317. Non-bank FIs have varying levels of internal controls in place, although it appeared that they were adequate in view of the risk and business conducted. They advised that human resources assigned to AML/CFT matters are generally limited.

318. Casinos appeared to have adequate internal policies and internal control procedures. These procedures take into account risk factors and examples when the application of simplified or enhanced customer due diligence measures must be taken. Casinos reported that training is provided for staff periodically.

319. Other DNFBPs (such as notaries, lawyers, real estate agents) indicated that they do not have AML/CFT compliance structures in place as the majority of them are sole practitioners.

320. All reporting entities notify the FIU in writing of the designation as well as replacement of employees responsible for AML/CFT functions and board members no later than seven working days from the date of their designation or replacement.

321. Most non-bank FIs and all DNFBP sector representatives reported that they need to develop their IT systems further and allocate more human resources to AML/CFT matters. Most of them claimed that they are satisfied with the training organised by their supervisors and/or the FIU but some real estate agents and traders over EUR 10,000 in cash indicated that they have never been trained.

322. There are no legal or regulatory requirements which impede the implementation of internal controls and procedures to ensure compliance with AML/CFT requirements. There are no legal or regulatory difficulties in the transfer of customer or CDD information between group entities.

Conclusion

323. **Lithuania has achieved a moderate level of effectiveness for IO4.**

CHAPTER 6. SUPERVISION

Key Findings and Recommended Actions

Key Findings

1. The BoL applies very good controls in relation to the licensing of FIs to prevent criminals from holding, or being the beneficial owner of, a significant or controlling interest or holding a management function in FIs. Controls in relation to DNFBPs vary, including an absence of registration requirements for TCSPs, real estate agents and accountants.

2. The BOL has a good understanding of ML risk within banks, and products and services offered by FIs and a general understanding of ML risks in the sectors it supervises. It appears generally to understand FT risk.

3. In general, DNFBP supervisory authorities except the FIU (which has a generally good understanding of the ML/FT risks of real estate agents and accountants) have a developing understanding of risk.

4. The BOL is a proactive supervisor and has increased the level of supervision significantly during the last two years. It has some strong elements of risk-based supervision and is moving towards both a comprehensive risk-based approach and an amount of supervision commensurate with risks; although, the shortage of staff resources has had a negative impact on the overall effectiveness of the risk-based approach to supervision.

5. With regard to DNFBP supervisory authorities, the extent of AML/CFT supervision and the degree this is risk-based varies, with the GCA, the FIU and the LAO being most proactive authorities; overall, risk-based approaches and the levels of supervision undertaken require improvement. Limited human resources have a negative impact on the supervisors' ability to perform their functions.

6. The level of sanctions applied by the BoL has generally been commensurate with its supervisory findings. There are very good elements of effectiveness and dissuasiveness although the regime is not yet fully effective and dissuasive.

7. Some sanctions have been applied by DNFBP supervisory authorities and the courts in relation to DNFBPs. Overall, the application of the frameworks and their effectiveness is at a relatively early stage of development.

8. Most supervisory authorities, most notably the BoL, were able to point to improvements in AML/CFT compliance as a result of their interventions. The BoL was able to demonstrate that it is making a significant difference.

9. The BoL and most DNFBP supervisory authorities have promoted understanding by supervised entities of their obligations and risks, albeit there is scope for improvement.

Recommended Actions

1. As planned, registration of TCSPs should be introduced and registration and standard setting frameworks should be put in place for real estate agents and accountants. The GCA should develop its existing approach, while other DNFBP supervisors should take additional steps to prevent criminals from holding, or being the beneficial owner of, a significant or controlling interest or holding a management function in DNFBPs.

2. Supervisory authorities should co-ordinate their individual approaches to addressing risk with a view to developing comprehensive risk-based supervision in all sectors covered by the FATF Standards.

3. The BoL and the FIU should use onsite and offsite tools, and the next iteration of the NRA, to enhance their understanding of ML and FT risks relevant to their sectors. Other supervisory authorities should use these tools and the NRA to develop comprehensive understanding.

4. The BoL should enhance its existing risk-based approach and further develop its ML/FT risk assessment in order to ensure that risk-based supervision is comprehensive. DNFBP supervisors should take the significant steps required to achieve comprehensive risk-based approaches to supervision. Systematic AML/CFT training programmes should be developed by the supervisory authorities.

5. The BoL should intensify its use of sanctions as its approaches to supervision develop and the amount of supervision increases so as to ensure that its sanctions framework is effective and proportionate. DNFBP supervisory authorities should ensure that they articulate their approaches to sanctions and that their imposition of sanctions is effective and dissuasive.

6. The BOL should enhance its existing outreach with FIs by issuing guidance. DNFBP supervisory authorities should consult with their sectors and issue relevant guidance.

7. All supervisory authorities should be provided with the additional budgetary and human resources necessary for effective supervision (including meeting the recommended actions above).

Immediate Outcome 3 (Supervision)

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

BoL

324. The BoL applies very good controls in relation to the licensing of banks and other FIs to prevent criminals from holding, or being the beneficial owner of, a significant or controlling interest or holding a management function in FIs. It is commendable that, consistent with risks, the BoL's operational risk and licensing divisions work closely together on these and other applications for licences. Fit and proper decisions are made through the EU Single Supervisory Mechanism (SSM) for members of the management board and supervisory board of the three significant banks in Lithuania,

and for qualifying shareholders of all banks[68]. Applications for all banking licences involve frequent communication with the ECB and the final decision is made by the ECB.

325. The BoL's scope has recently widened to cover companies engaged in business using various developing technologies; the BoL pays particular attention to the licensing of these businesses and seeks to ensure that only good quality businesses enter the market. The AML/CFT team in particular devotes considerable time to assisting the licensing division, for example, to understand the risks of applications involving developing technologies. There are particular challenges in dealing with such applications and the licensing process is longer than for other FIs. These challenges include the quality of the application and business proposal, understanding of risk by the sponsors, the entrepreneurial nature of what is proposed, and potential controllers who are new to regulation. The cultures of developing technology sectors are significantly different from that of the banking sectors but the BOL is successful in managing these differences. Part of the management process includes the BoL's participation in Lithuania's "new-comers' programme" established to promote developing technology and which is used by the BoL to meet prospective applicants for a licence and explain its requirements at the earliest opportunity. The BoL also liaises with the Commission for National Security on country risk, which provides valuable information on the reputation and bona fides of persons in the ownership structure or involved with applications.

326. The licensing division (which is separate to the AML/CFT division) comprises 12 officers and it liaises with other divisions of the BoL (including the AML/CFT division) to ensure a joined-up approach and the maximum amount of information and analysis for its decisions on licensing. It has licensed a large number of Fintech, e-money and payment institutions and payment platforms (and other non-bank entities) in the last two years. It has been some years since an application for a full banking licence was received although at the time of on-site visit it was dealing with three applications for special purpose banks (which cannot provide investment services).

327. The full ownership structure of applicants is reviewed. Legal and beneficial owners who meet the 10% threshold at each level of ownership are subject to assessment (the threshold is 20% for a few types of non-bank FIs). The checks by the BoL also seek to ascertain whether persons under the threshold are acting in concert, which would be deemed as crossing the threshold. Such relationships have been found as a result of scrutiny of copies of written agreements between owners and scrutiny of the totality of the application (e.g. where separate investors in the applicant have the same beneficial owners). Shareholders and owners meeting the threshold throughout the layers of ownership are subject to analysis of their reputation and their financial status, including source of income. ECB approaches are closely followed but the BoL requires further information than that articulated in ECB guidance. The BoL takes as long as is necessary to complete its checks.

328. Application material provided to the BoL is divided into four parts, namely reputation, proof of source of funds, financial statements and proof of absence of a criminal record. Additionally, the BoL receives material describing the FI`s proposed business model and controls (such as the business plan and AML/CFT policies and procedures) in order to assess the readiness of an applicant to implement adequate AML/CFT controls.

329. Financial statements for the last two years are required and checked against local registers and the tax authority's records. In order to ensure that information provided on the source of funds is

[68] The ECB has the power to make fit and proper decision only for the banks which are considered as significant. The BoL is responsible for fit and proper decisions in relation to less significant banks.

sufficient and credible, the BoL requires financial statements to be provided to it from, and approved by, the state tax authority. Other documentation is also required, such as an extract from the public register of real estate (where relevant) and information on: other investments (stocks, deposits etc.), bank accounts and any companies owned (and their financial status). In some cases the applicant must provide additional explanations regarding the source of funds by, for example, providing and explaining contracts and agreements. There would be merit in also exploring whether there are cross-linkages between elements of the information.

330. Internal procedures for AML/CFT and other control purposes are obtained and assessed against the proposed business model. The AML/CFT division of the operational risk division also engages in in-depth assessment the adequateness of controls and procedures corresponding to the business model. Media and internet checks are routinely undertaken for every application and checks are conducted with a wide range of other authorities in Lithuania (LEAs, the FIU, the security services, the special investigations unit, the anti-corruption agency, the MoI's national database and the National Registry). A private company is also used to complement the BoL's due diligence and verify information such as whether there are disputes or insolvency proceedings. Information on qualifications, including copies of diplomas, is verified on a risk basis by referring the applicant to the Centre for Quality Assessment in Higher Education to validate qualifications awarded both within and outside Lithuania. This has led to inconsistencies being uncovered. Interviews are not only held as part of the newcomers programme but, in addition, when considered necessary on other occasions. Information is also requested from foreign authorities and the BoL has demonstrated its significant efforts in this regard; responses are received on most occasions. Non-responses are followed up when there are negative indications from other sources. Once the entire package of information for an application has been collected, in each case the BoL decides whether the collected information is sufficient to issue a licence. Beneficial owners outside Lithuania are rare except in relation to Fintech companies and any gap in follow up of requests would not appear to be significant. Nevertheless, there would be merit in extending the follow up process where foreign authorities do not respond to requests for information.

331. While the overall approach for each type of licence is consistent, each sector's application form is different and each application is addressed on its own merits; the information required and assessment of it are tailored accordingly. For individuals, references from previous employers are not required and (noting the information offered by contact with foreign authorities and due diligence reports in relation to employment history) there might be merit, on a case by case basis, in considering whether obtaining references would be useful.

332. The same approach as that outlined above is applied to legal owners and senior managers.

333. All applications are provided with a risk rating linked to the business model and purpose of the applicant. As part of this, consideration is given to ML/FT risk; geographical risk of the jurisdictions to which (and from which) payments will be made; the geographical risk of the beneficial owners, owners and managers (for example, citizenship, place of residence, links with other higher risk countries or jurisdictions); negative information on managers, shareholders and previously owned companies; the proposed customer base; business channels used to reach customers (for example, delivery channels and marketing channels); ML/FT risk of financial products and services; and legal risk. Using this risk model to help focus consideration of the application is a positive development by the BoL. The process is not articulated in writing and the risk rating process would benefit from formalisation and automation and from carrying the rating and underlying risk

assessment through to the rest of the BoL's AML/CFT work.

334. Payment institutions take advantage of EU pass-porting mechanisms to undertake business in Lithuania. Hence, there are a number of money services businesses (MSBs) which have notified the BoL that they are operating in Lithuania for which another supervisory authority in another EU Member State is responsible.

335. Although there has been only one refusal of an application for a licence since the beginning of 2016, the BoL provided 8 examples where applications have been withdrawn (some 9% of the total) as a result of the robustness of its checks.

336. Analysis of individuals' connections is part of the assessment process and the overall range of checks is such that, in practice, they comprise scrutiny of whether a person is an associate of a criminal.

337. Changes of owner, beneficial owner or senior manager have to receive prior approval from the BoL. The BoL routinely checks information in the National Registry of Shareholders and the media against its records. On a few occasions, its checks at the registry have uncovered situations where changes have not been advised. The normal consequence is a warning but fines have also been imposed.

DNFBP supervisors

338. Casinos are subject to licensing controls. Although there is some over reliance by the GCA on checks undertaken by the FIU and other third parties the overall controls are good quality. Information is received by the GCA on directors, senior managers and beneficial owners.

339. There are five staff in the GCA's licensing department. Material provided by applicants includes data on the company's supervisory board such as identity details of members of the board, the head of administration, his/her deputy, the chief financier; the participation of these persons in the management of other companies; information on the source of funds of the applicant such as loans, donation contracts, agreements, bank accounts, income declarations, a statement of wages from the employer and other relevant documents, which depend on what the applicant indicates as a source of funds. Identification data for legal and beneficial owners, and their source of funds, is also required.

340. The GCA analyses the application material as well as the conclusions of the authorities from which it has sought input. It checks the National Registry of Shareholders, and registers of suspects and accused sentenced persons. It has also contacted authorities in other jurisdictions, such as tax and gambling authorities, for input where shareholders, members of the company's supervisory board, the head of administration, his deputy, the chief financier or beneficial owner is a resident of the foreign country. In addition, the GCA contacts the MoI to ascertain whether the persons mentioned above have criminal records in Lithuania. Three individuals were detected as having received criminal records prior to their appointment at casinos and the individuals, at the casinos responsible for hiring/employment of the individuals were sanctioned by fines. The GCA also sees this as an indirect sanction on the relevant casinos. It provides all of the application material to the Police, the FIU and the Security Services to be checked (this must be done within three days of receipt of an application). In addition, also within three business days of receipt, the GCA must submit the copies of all documents and information to the territorial state tax inspectorates and the relevant territorial office of the State Social Insurance Fund Board to ascertain, for example, whether the applicant owes tax to the state budget or municipal budgets or state money funds. These deadlines are overly restrictive.

341. The GCA has the right to request additional documents and information no later than within five working days from receipt of the documents and information if they are necessary to make a decision to issue a licence. This deadline is also overly restrictive. A decision on whether or not to issue a licence must be taken by the GCA within 30 days of receipt of all documents and information. While, there have been two applications in recent years which have generated particular consideration (where the founders of the applicants were foreign companies and it was difficult for the GCA to confirm the beneficial ownership), the issues were overcome. The 30 day deadline has therefore not been a problem in practice and the GCA has confirmed that, where it is not satisfied within that timeframe, it would not issue a licence. Nevertheless, the evaluation team considers that there would be merit in establishing a less restrictive statutory approach.

342. The GCA must be advised of changes to legal or beneficial ownership within five business days of the change. Approximately every three months the GCA takes the positive step of checking the ownership details of casinos at the National Registry; on occasion it has uncovered cases where it has not been advised of changes. Overall, once or twice a year the GCA is not advised of changes which have been made. Sanctions have not been issued. Instead, letters have been sent to the casino in question reminding it of its statutory obligations under the Gaming Licensing Rules. There has been no general communication with the casino sector to remind it of the obligation to report changes.

343. The GCA's checks would go some way to ascertaining whether individuals are associates of criminals (although the statutory framework does not address associates of criminals).

344. Before they are permitted to undertake their professional activities notaries are required to make an application to the MoJ and provide a confirmation of non-conviction from the MoI. The assessment team did not meet the MoJ and has not been advised of any specific checks or whether any applications have been refused. In 2017, one notary was dismissed by MoJ on the basis of the notary committing a serious crime. In other cases, which occurred in last three years, notaries were dismissed by MoJ on other bases, including three or four cases where the notary was considered unsuitable to hold office.

345. Every advocate must be a member of the Bar Association and meet the Association's requirements. A confirmation of non-conviction from the MoI must be provided to the Bar Association as part of the application to be an advocate. The Bar Association checks the internet on a risk basis, namely where the applicant is known from the media or has negative connotations. In addition, the Bar Association has sought input from the FIU on a few occasions. No applications were rejected in 2016; one application was rejected in 2017. The Bar Association has been able to delist advocates for a combination of financial crime convictions and failure to meet the legal test of high moral character.

346. DPMS must notify the Lithuanian Assay Office (LAO) of their existence by providing it with the name and address of the dealer, together with the names of the directors and their dates of birth. Although the LAO maintains a register, it does not undertake checks. The LAO is of the view that the information it receives from the police, the FIU and the public suggests that all DPMS are currently registered. Dealers which the LAO considers to be acting illegally (i.e. without having made a notification to it) are reported to the police and a joint inspection is made to the dealer (11 since the beginning of 2016). The LAO and the police do not liaise to discuss case developments – four of the joint inspections have led to administrative proceedings. Joint inspections have also been undertaken with the tax authority and with customs.

347. TCSPs, real estate agents and accountants are not subject to a registration requirement

(although TCSPs will be subject to registration requirements under the FIU's responsibility from August 2018. It considers that most TCSPs are lawyers. The FIU checks whether the beneficial owners, owners and senior managers of the DNFBPs for which it is responsible have criminal records as part of its onsite inspection process. The FIU considers that it has records of some 70% of real estate brokers; it is not in a position to estimate a percentage for accountants. The introduction of legislation and the establishment of a supervisory body for accountants to set standards would be beneficial.

Supervisors' understanding and identification of ML/TF risks

348. In the view of the assessment team, the information in the NRA has not added meaningful value to the supervisory authorities' understanding of risk in relation to the sectors they supervise and this can only reduce understanding of risk.

BoL

349. The BoL has a good understanding of the overall and ML risk cultures within FIs, and products and services offered by FIs, but it can have only a general understanding of ML risks in the sectors it supervises in light of the issues raised in IO.1. It considers banks have a good risk culture and understanding of risk, and that this in turn benefits understanding by the BoL (other FIs have a less sophisticated culture and a lesser degree of understanding). The depth of the BoL's licensing controls have a positive, impact on the understanding of risk of market participants and their level of AML/CFT controls.

350. The BoL holds annual compliance meetings with all FIs (and additional routine meetings with banks); it is also in routine communication with the FIU, which informs the BoL's views on risk. The BoL was convincing about its understanding of the risk arising from developing technologies. In light of Lithuania's drive to increase business in this area, the BoL has sought to understand the risks as much as possible. It has a general understanding of the risks of offshore finance centres, e-money institutions, the risk of the real estate sector to banks and cash transactions (the BoL has conducted a thematic review of use of cash in banks, it receives reports from all currency exchange operators every six months, and it has a focus on cash in inspections). It also has a general understanding of the risks to banks arising from legal persons and the different risk appetites of banks in relation to legal persons; the risks arising from offshore finance centres (i.e. foreign legal persons) are decreasing. The BoL has sufficient knowledge of banks' approaches to leverage their understanding. The BoL was also aware of the approaches by non-bank FIs to addressing risk and the risk profiles of these FIs.

351. The implications to Lithuanian banks of the "laundromat" case have also been proactively investigated. During 2009-2011 the BoL's supervision led to the provision of information by it to the FIU in relation to potential criminality at two banks. Criminal proceedings were initiated. These are still ongoing.

352. The banks became bankrupt in 2011 and 2013 respectively (see Boxes 7.3 (Bank Snoras) and 7.4 (Ūkio bankas) in IO.7). The majority of non-resident customers using Lithuania were concentrated in these two banks and their collapse contributed to the significant decrease of non-resident business in the country. A small proportion of the non-resident customers from the two banks transferred their business to a few other Lithuanian banks (mainly as this retained their entitlement to compensation of up to EUR 100,000). The BoL routinely monitored all changes of the

non-resident customer portfolios held by the remaining banks. For example, up to April 2014 all banks were required to provide daily reports containing key information on assets and liabilities; whenever there were any tangible changes to the volume of deposits, banks were required to provide further, detailed, information on transactions. In addition, after the collapse of the two banks, the BoL undertook AML/CFT on-site inspections to all banks and branches that had increased their non-resident customer portfolios (this was primarily attributable to previous customers of Ūkio bankas) and all banks and branches which shared any similar patterns of business to those in the "laundromat" case. During these inspections, banks were able to demonstrate their understanding of risks and no significant AML/CFT breaches were identified in most of the banks (in one case a bank was sanctioned - this was nothing to do with the case). Throughout the period from 2009, the BoL also liaised with the FIU both in relation to progress of the criminal proceedings and to monitor intelligence on the banks that were inspected afterwards; all onsite inspection reports were provided to the FIU.

353. Following media reports in 2017 about Lithuanian involvement in the "laundromat" case, the BoL investigated the matter again. It liaised with the FIU and contacted all banks to obtain information in relation to customers and the banks themselves, and any direct or indirect involvement in the case or persons linked to the case. The banks` responses were also provided to the FIU. The BoL concluded that further action was not necessary as the investigation confirmed the majority of relevant funds went through Ūkio bankas and that there was no new information to be uncovered – some clients of Ūkio bankas had already been under investigation for ML since 2013. The information in the media was already known to the BoL and the FIU. There is no intelligence or other information to suggest that existing Lithuanian banks played any part in the case. The number of legacy customers and transactions remaining from the two banks involved in the case is limited, and the risks of those customers are understood.

354. FT risk is generally understood but needs more refinement than understanding of ML risk. The BoL does not separate FT from ML risks in its supervision but has sought through its offsite questionnaires to establish whether banks' overall classification of risks is adequate. This includes information on the number of transactions and amounts transmitted to and from countries near conflict zones. The BoL had a general understanding of country risk but it needs to carry out more assessment of risk in this area from a FT perspective (including in relation to NPOs notwithstanding questions on NPOs which were included in the off-site questionnaires in 2017 and 2018). This general understanding held by the BoL is supported by the discussions the assessment team held with banks on their processes and countermeasures. In addition, FT risks arising from foreign MSBs using EU pass-porting provisions to undertake business in Lithuania need to be better assessed and understood. A clearer jurisdictional framework for TFS will also aid the BoL's understanding of FT risk. It risk needs to be assessed separately to ML risk so that the BoL can obtain a fuller understanding of FT risk and so that conclusions in the next iteration of the NRA can be supported. More generally, the questionnaires issued to banks and other financial market participants do not have a focus on FT risk and it would, therefore, be beneficial to extend the scope of the questionnaires.

DNFBP supervisors

355. DNFBP supervisory authorities except the FIU (which had an overall good understanding of the ML/FT risks of real estate agents and accountants) do not have a developed understanding of risk.

356. The FIU considered real estate agents to have higher ML risk in light of the significant number of property transactions involving cash; it also sees links between this and corruption by, for example, PEPs. While it does not receive STRs from the sector, it does receive CTRs. This suggests to the assessment team that more emphasis should be given to improving standards for the reporting of suspicion. In the absence of the ML indicators, accountants are considered to present a much lower ML risk than estate agents. It is not considered real estate brokers or accountants present a risk of FT as there is no intelligence or evidence of these reporting entities bring engaged in FT. In addition to its sectorial understanding, the FIU had a good understanding of the risks of individual institutions which it had inspected.

357. The recent issue of a questionnaire has focussed the GCA's thinking on ML/FT risk. It has reviewed all responses and this, together with its onsite inspections, provides it with some knowledge of the risks of individual institutions. Only cash can be used to purchase chips in casinos but risk is increased as exchange services are allowed. The GCA is also of the view that remote identification by e-casinos presents risk; the funds deposited with e-casinos by customers are not seen as presenting inherent risk as the funds are provided from bank accounts by use of credit cards. Overall, the GCA's understanding of risk is developing.

358. The Chamber of Notaries considered that the most significant ML risk to notaries would arise from criminals taking out a loan and repaying the loan in cash. This is one of several red flags for notaries where the risk of a "simulated transaction" might arise. The assessment team notes that notaries must always be used for real estate transactions and that customers can enter bank premises and deposit funds directly in a notary's bank account without recourse to the notary. In practice, the use of notaries' deposit accounts, whether directly by the notary or otherwise, is not common, with transfers taking place on 503 occasions in 2017 out of a total of 1,702,683 notarial acts in that year. The Chamber was not aware of the typologies contained within STRs made by notaries. Overall, the Chamber's understanding of risk is developing.

359. The Bar Association considered that the position of advocates in relation to customer relationships indicated a minimal ML/FT risk for the profession. The assessment team cannot agree with this conclusion in the absence of evidence to support it.

360. The LAO sees the main risks as being the lack of knowledge and understanding by DPMS of AML/CFT problems and cash operations (particularly cash operations in smaller shops). At the time of the visit it considered that these risks were mitigated as it receives information from Customs on the names of all importers and exporters of precious metals and stones. All importers must be registered at the LAO. There are fifteen examples since the beginning of 2016 of Customs refusing the importation of precious metals and/or stones where the importer/exporter was not registered. The LAO also noted that most transactions are only for small amounts of metal/stones. Non-resident purchasers from Belorussia are reasonably common. The LAO estimated that the split between the number of cash and credit card purchases was approximately the same. The assessment team also characterises the LAO's views on risk as developing.

Risk-based supervision of compliance with AML/CTF requirements

BoL

Introduction

361. The AML/CFT division is part of the operational risk division (which is itself one of several

divisions with supervisory responsibilities) of the BoL and has recently increased from three to five staff. It appears to the assessment team that the shortage of resources has had an unfavourable effect on the on-site and offsite supervision undertaken during the period under review: the number of market participants (specifically in the e-money/payment sector) increased significantly in 2017 compared with 2015; on occasions the number of customer files sampled during on-site inspections should have been higher in order to form a more complete picture of FIs' risks and the appropriateness of AML/CTF controls; and the thematic reviews have in some cases lacked in-depth analysis. The AML/CFT division has prioritised its work (for example, focussing on banks with a high ML threat but weaker controls). The BoL is of the view that, during the period under review, the pattern and number of on-site inspections were adequate as the priority was given to the riskier FIs, noting that the majority of licensed institutions were e-money institutions and that these did not undertake significant activities in 2017. As a formal and comprehensive risk-based system is not yet in place, the assessment team is of the view that the number and pattern of onsite inspections cannot be demonstrated as being fully consistent with that system and, while noting the increase in the number of inspections from 2017, it retains a concern in this regard, particularly in relation to banking sector entities in the period under review (also see the table below). The assessment team considers that, once the two new staff have been trained and integrated within the division's work, a further, but not substantial, increase will be necessary to undertake comprehensive risk-based supervision (and address the other matters raised in this IO). The introduction of a programme of systematic training would also be beneficial. The BoL's policy team would also benefit from additional resource.

362. The AML/CFT division has steadily enhanced its supervisory approach over the last two years and has some strong elements of a risk-based approach to AML/CFT supervision. During the period under review, it has undertaken onsite inspections, with a focus on banks and high risk e-money and payment institutions. Onsite inspections to these and other FIs are undertaken by the AML/CFT division, devoted to AML/CFT, strong in their coverage of ML and concentrate on risk to a significant degree. While performing offsite supervision the BoL uses an annual questionnaire, which includes quantitative data on e.g. geographical risk, client risk, product/service risk, and delivery channels risk, as well as qualitative data on internal controls. Additional information is gathered from prudential supervision. In addition, thematic surveys in line with Lithuania's risks have been carried out to better understand and address risks in relation to offshore jurisdictions, cash transactions and payment and e-money institutions. Staff are proactive, and the operational risk division has worked effectively during the last two years within what has been a significant shortfall in staff.

BoL - The Wider Approach and AML/CFT Links

363. The BoL has an overall approach to addressing risk (the Risk-Based System Concept). It allocates FIs to four sectoral categories with the aim of distributing its overall supervisory resources so as to pay more attention to the largest market participants, whose activities are potentially (but not necessarily) subject to higher ML risks. The first category of FI (banks) is subject to enhanced supervision, which includes analysis of quarterly off-site reports on AML/CFT controls (such as AML/CFT risk analysis reports and audit reports) that supplement the annual questionnaire on ML/FT risks. Also, compliance meetings with each bank's management are carried out at least annually during which supervisory issues (including AML/CFT) are discussed. FIs within the second category are those whose activities might have risk but which do not raise major concerns (e.g. due to a small market share). Therefore, they are subject to less intense supervisory action. Nevertheless, like all other FIs, they are subject to reporting on AML/CFT risks via completion of the annual

questionnaire.

364. While deciding on the frequency and intensity of supervisory engagement both the sectoral categories and the risk of individual FIs are considered by the BoL. While formal AML/CFT risk ratings are allocated to banks, the purpose of this is to inform, and be part of, the overall operational risk rating (i.e. while deciding on the operational risk rating, ML/FT risks as well as gaps in the AML/CFT controls are taken into account). In addition, the AML/CFT division uses that rating and the analysis underpinning it to inform its approach. In addition, the division has a conceptual and informal AML/CFT risk rating for other FIs, which also informs its approach (e.g. two e-money institutions considered to be high risk have been subject to onsite inspections). While deciding the risk of each FI, factors such as the risks of the services provided, the jurisdictional risks of the residence and place of citizenship of beneficial owners and senior managers, and their links with other companies, the quality of AML/CFT measures are considered, although not articulated in writing.

365. Supervisory plans are prepared each year by the BoL including but not limited to on-site inspection plans. A range of risks, not only those related to AML/CFT, are considered to form a decision on what FIs should be inspected. The BoL aims to inspect banks at least every two to five years (based on the risks identified, the frequency of inspections might be increased), while other FIs are subject to on-site inspections based on risk analysis. The discussions on the ML/FT risk of individual institutions are not yet formalised, structured or articulated. Although the overall process has merit in generating discussion and the AML/CFT elements are taken seriously, the introduction of a methodological guide on how to establish and apply an AML/CFT risk rating for different institutions, as well as automated data analysis and risk scoring tools, would be beneficial for the BoL.

BoL - AML/CFT Division

366. The AML/CFT division works within the BoL's approach to risk and supervision outlined above, and also complements this approach in its day to day operations. Where the division concludes that an AML/CFT onsite inspection should be undertaken as part of the BoL's annual plan (which is published), it is successful. Ad hoc inspections are also undertaken; these are driven by a combination of intelligence received by the AML/CFT division from prudential supervision or market conduct supervision of the BoL. Ad hoc inspections in 2017 significantly increased the number of inspections undertaken in that year but they were not undertaken in the two years prior to that. Taking into account the significant involvement of the AML/CFT division in the licensing process, the lack of efficient offsite processes (labour-intensive/time-consuming/lacking automated tools), together with the increasing number of applicants for licences and the increasing number of operating FIs, it appears to the assessment team that the BoL cannot to meet its goal of inspecting all banks within the five year period specified in its risk-based supervision concept methodology (during the timeframe 2014-2019) with the resources it has. The table below provides information on the number and pattern of onsite inspections by the BoL from 2015 to the assessment team's visit to Lithuania.

Table 21: On-site inspections and sanctions issued by the BoL (ordered by type of FI)

Type of FI	Name of FI	Reasons for on-site inspection	Planned/ad hoc inspection (including follow up inspections)	Sanctions imposed by the BoL	Year
Banks	A	Regular on-site visit as required by Risk-Based System Concept (RBSC)	Planned	*	2015
	B	Higher AML/CFT risk FI (based on offsite information)	Planned		
Banks	M	Regular on-site visit as required by RBSC	Planned	1 written warning for the first bank and publicising of the sanction on the BoL website. 1 fine of EUR 235,350 and a requirement for the second bank to eliminate the deficiencies, while lending was temporarily restricted. The fine was publicised on the BoL website.	2017
	N (including MVTS services; money remittance services were included in the scope of on-site)	Higher AML/CFT risk FI (based on offsite information)	Planned		
Foreign bank branches	K	Higher AML/CFT risk FI (based on offsite information)	Planned	All findings of on-site inspections (to the two largest foreign bank branches) were notified to the home supervisory authority. Information was publicised on the BoL website.	2016
	L	Higher AML/CFT risk FI (based on offsite information)	Planned		
Life insurance	C	Higher AML/CFT risk FI (based on offsite information)	Planned	*	2015
	O	Higher AML/CFT risk FI (based on offsite information)	Planned	1 written warning, including publication on the BoL website	2017
E-Money Institutions (EMI)	D	Higher AML/CFT risk FI (based on offsite information)	Planned	1 fine of EUR 11,674 including publication on the BoL website	2015
	I	Higher AML/CFT risk FI (based on offsite information)	Planned	1 written warning, including publication on the BoL website	2016
	U (including MVTS services; money remittance services were included in the scope of on-site)	Higher AML/CFT risk FI (based on offsite information)	Planned	1 written warning, including publication on the BoL website	2017
	V	Trigger from external source (whistle blower)	Ad hoc	Fine of EUR 700,000 for the FI and fine of EUR 500,000 for the director,	2018

Type of FI	Name of FI	Reasons for on-site inspection	Planned/ad hoc inspection (including follow up inspections)	Sanctions imposed by the BoL	Year
				including publication on the BoL website	
	D	Higher AML/CFT risk FI (based on offsite information)	Planned (follow- up)	*	
	I			Fine of EUR 30,400 including publication on the BoL website	
Financial brokerage firms	E	Higher AML/CFT risk FI (based on offsite information)	Planned	2 written warnings, including publication on the BoL website	2015
	F				
	P			*	2017
Credit unions	G	Higher AML/CFT risk FI (based on offsite information)	Planned	1 moratorium (suspension of activities), including publication on the BoL website	2015
	Q	Trigger from prudential supervision	Ad hoc	3 written warnings and 1 moratorium. The sanctions were publicised on the BoL website	2017
	R		Ad hoc		
	S		Ad hoc		
	T		Ad hoc		
Payment institutions (money remittance services were included in the scope of on-site)	H (3 more entities were sanctioned for failing to provide information though not inspected; The "U" entity was sanctioned for failing to provide information as it sought to upgrade its licence to EMI)	Higher AML/CFT risk FI (based on offsite information)	Planned	1 fine of EUR 19,731 for failing to provide information on change of manager; 1 written warning for failing to provide information on change of manager; 1 suspension of voting rights of shareholder due to not meeting the reputation requirement, and publication on the BoL website	2015
Payment institution	J		Planned	*	2016

* An Order of the BoL to eliminate the deficiencies identified during an on-site inspection is issued when shortcomings of a minor nature are identified. Orders are obligatory and require supervised entities to eliminate the deficiencies identified during the on-site inspection within a specific timeframe.

367. There is some change of intensity of onsite supervision as between sectors and firms in that the number and type of customer files sampled differs as between FIs inspected and information in one file can, and does, lead to other, linked, customer files being sampled. The selection is based on

the information considered from off-site supervision and judgement (based on the experience and knowledge of the inspection team). There have been situations where more files could have been selected in order to form a complete picture of FIs' systems.

368. During an inspection the BoL is able to receive copies of STRs if it selects the relevant customer file for review. Otherwise, it is not provided with STRs. The reduction in the effectiveness of supervision is mitigated to some extent in that the BoL is provided with information on unusual transactions and internal assessment of those transactions, and where there is an internal investigation, and an STR is not made, it assesses the FI's decision-making process.

369. Off-site supervision has developed since 2014. A pilot questionnaire to banks in that year was followed in 2015 by a more detailed questionnaire seeking information on technical compliance and internal controls, together with a few questions on risk. In 2016 the questionnaire was issued again but with an enhanced statistical component. In 2017 a further (but different) questionnaire was issued to seek information on risk via statistics and self-assessment responses to questions. Additionally, the BoL receives information from all banks including on (but not limited to) AML/CFT controls on a quarterly basis. This information is based on what individual banks have in place in practice (management protocols, audit reports, compliance reports, risk reports, etc.).

370. In addition, in 2016 the BoL carried out themed exercises to understand the risks arising from the Panama Papers, risks in the payment sector, and the risks of cash transactions. This continuous development of approach and the themed exercises are commendable. This offsite supervision has led the BoL to apply enhanced supervision to two FIs. Nevertheless, a shortage of staff resources has meant that more work still needs to be done to formally assess and understand the results of the cash transactions exercise and this also means that the assessment team has a concern that the assessments of the other two exercises would have been more developed if sufficient staff resources had been available.

371. The BoL liaises with the FIU routinely to inform its supervision (e.g. there has been discussion of risks in general and in relation to particular FIs, suggestions made by the FIU as to which FIs would benefit from an inspection) and annual inspection plans and inspection reports of individual FIs are shared by the BoL with the FIU. From time to time (in 2013, 2017 and 2018), the FIU has joined the BoL's inspections. This liaison is positive and beneficial to both authorities.

BoL - FT

372. Supervisory controls are not as well developed for FT risk as compared with ML risk. This is the result of the low risk rating provided for FT in the NRA.

DNFBP supervisors

373. With regard to DNFBP supervisory authorities, the extent of AML/CFT supervision and the degree this is risk-based varies; none of these authorities has a comprehensive risk-based system. The GCA, the FIU and the LAO have been the most proactive authorities (the sectors supervised by the GCA and the LAO being the highest risk DNFBP sectors from the perspective of the FIU and the Police). DNFBP supervisors need further staff resources and would benefit from the establishment of programmes of routine, systematic AML/CFT training; currently there is reliance on training by the FIU. The number of onsite inspections by DNFBP supervisory authorities indicated in the table below.

374. The GCA assumed responsibility for the AML/CFT supervision of casinos in the summer of 2017 and has 27 staff; four of these specialise in AML/CFT supervision. Training of GCA staff is

undertaken but focuses on technical gambling requirements rather than on AML/CFT. The GCA has sought to ensure that it can address the challenges of e-casinos by this training, by its direct access to the databases of e-casinos and through the inspection process. While its knowledge is developing, there is a need to introduce a systematic training programme to cover AML/CFT in relation to both physical casinos and e-casinos.

375. There has been a significant number of onsite inspections to casinos in the last two years. All onsite inspections cover AML/CFT but, of the 14 onsite inspections in 2014 and 19 in 2015, three and five respectively, were dedicated to AML/CFT. All casinos were inspected in relation to AML/CFT in 2016. E-casinos have been permitted since 2016. Four of these were inspected by the FIU in 2017 at the request of the GCA (all four received sanctions from the Court), with one e-casino being subject to inspection by the GCA in 2018 following receipt of a complaint on the identification process by a customer. The attention paid by the GCA to recognising and addressing the risks presented by e-casinos is positive. While the GCA did not have robust enforcement powers until the summer of 2017, it was nevertheless able to creatively leverage the responsibilities and enforcement powers of the FIU to undertake inspections where sanctions might be needed. Other inspections have been carried out by the GCA in conjunction with the FIU. It would be beneficial for as much as possible of the GCA's future training programme to involve the FIU as it has also not undertaken specific training on AML/CFT in relation to casinos.

376. Inspections were narrowly focussed until the summer of 2017, concentrating on the register of customers, how casinos identified customers and the checks undertaken for stakes of greater than EUR 1,000. While the focus is still relatively narrow, since the summer of 2017, the GCA has also paid more attention to customer due diligence and checked all four registers required to be maintained by casinos (customers entering the casino, customers making deposits and collecting wins, customers with terminated transactions/relationships and STRs). Although not comprehensive, some practices onsite have evolved as a result of risk. For example, more attention is paid to cash operations and occasional customers. Typically, inspections are undertaken by two staff from the control department and two representatives of other departments, for example, to check compliance with technical gambling requirements. Each inspection takes the same period of time, and follows the same format, with some two hours spent in a casino (including online casinos). Inspection findings have informed to some extent the further actions taken by the GCA with, for example, a few casinos being inspected more than once.

377. The methodology for establishing the inspection plan is partially AML/CFT risk-based. It is predicated on risk criteria (including suspicion), the number of violations of the AML/CFT Law; repeated violations; problems with gaming devices; violations of legal requirements; and the scope of activities. Triggers for ad hoc inspections have included receipt of complaints from customers and other casinos, and information seen at one inspection linking the casino being inspected with another casino. It is intended to establish an AML/CFT risk-based approach to the inspection plan for 2018, informed by responses to a recently issued AML/CFT questionnaire sent to all supervised entities and, also from early 2018, receipt of AML/CFT procedures manuals and changes to the manuals. This was the first dedicated AML/CFT offsite supervision carried out by the GCA although general questionnaires had been issued since 2015 and these had included a few questions relevant to AML/CFT. The 2018 questionnaire covers questions on customer identification, monitoring, suspicion, registers maintained, cash transaction reporting, responsibility for compliance, training and polices and controls. The responses had been analysed and, while not leading to inspections in themselves, had informed the content of inspections. The assessment team welcomes this proactivity

and recommends that offsite supervision should be maintained; the GCA should also consider how it should best capture FT risk as its supervisory model develops.

378. The close level of cooperation between the GCA and the FIU has informed and enhanced the approach of both authorities. This will be especially valuable as the GCA moves towards a comprehensive risk-based approach.

379. With the inclusion of all gaming operations in the AML/CFT framework in 2017, the number of obliged entities has increased significantly and the GCA requires a significant increase in staff resources to undertake its responsibilities. This would allow for more detailed inspections and for these inspections to be undertaken on the basis of risk.

380. The FIU's analysis and compliance units are involved with the supervision of real estate agents and accountants. The number of inspections planned each year is limited by staff resources although, ad hoc inspections are undertaken. In the absence of a register of DNFBPs, the FIU forms views on which sector to inspect from when the sector in question was last subject to inspections, whether the sector is new, information in public sources such as the media, and intelligence received by the FIU. The selection of firms is based on receipt of complaints and information about potential illegality or non-compliance with legislation; and ensuring that violations found during pervious evaluations have been remedied. The FIU has undertaken follow-up inspections, depending on the severity of any problems found.

381. Inspections by the FIU in 2017 focussed on cash transactions in the casino, currency exchange and car dealer sectors, following the establishment of a significant number of currency exchange operations and the use of cash in real estate transactions. Casinos were selected on the basis of which casinos generated the largest number of STRs and concerns expressed by the GCA. At the time of the assessment team's visit to Lithuania, the FIU was engaged in a programme of inspections to accountants as the sector had not been visited for some years and participants are not aware of their AML/CFT obligations. It is not able to inspect more than two real estate agents in 2018. The FIU considered that the notary sector has increased in risk due to some deficiencies in verification of beneficial ownership, and so will be the subject of the next inspection plan.

382. Breaches at the previous onsite inspection, together with documentation and responses to questions, are considered before undertaking an inspection. The questions asked are different, depending on the sector and the DNFBP. Inspections last approximately half a day and are guided by a basic checklist. In addition, the FIU focuses attention on risk. The approach to each inspection is the same although the intensity of supervision changes as between entities to some extent, depending on the DNFBP being inspected. Differences include the number of customer files sampled a focus on the higher risks to the DNFBP such as customer relationships with high risk countries, PEPs and cash. This is consistent with Lithuania's risks. Some 20-50 customer files are sampled. The coverage of each inspection is wide.

383. The LAO has undertaken a significant number of inspections, albeit that it advised that these cover only whether all cash transactions have been registered; whether the number of transactions looks reasonable; training; whether dealers have AML/CFT procedures (the procedures are not assessed); and whether they know the requirements. Only the first and last of these factors are included in the questionnaire used by the LAO to guide the format of inspections. To date all dealers have maintained a register. Typically, one officer inspects a small shop, with two officers visiting larger premises, with inspections taking a few hours. Over 400 inspections are undertaken each year. During 2016 and 2017 eleven inspections were carried out jointly with the police, three with the tax

authority and two with Customs (reflecting the good relationships which the LAO has with these authorities). New businesses receive the questionnaire for completion instead of receiving an inspection; in addition, the LAO adopts this approach with some of the more established dealers which have been assessed as low risk-based on a document on the selection of criteria for selection of economic entities agreed in 2015. These criteria are mostly not specifically aimed at AML/CFT but intelligence from the FIU is included and some other elements are partly relevant for AML/CFT purposes.

384. The Chamber of Notaries indicated that two or three members of staff participate in inspections, which last some three hours. An inspection is normally scheduled for the first year of operation of a notary and then within every five years. It carries out a relatively small number of AML/CFT inspections on an ad hoc basis. These include a focus, inter alia, on reporting of suspicion although the overall coverage of inspections is not comprehensive. Decisions on which notaries to inspect are taken on the basis of complaints received and whether the Chamber's assessment commission has formed a view that a particular notary should be subject to inspection. Follow up inspections are also undertaken. Partial offsite supervision is also undertaken through surveys issued every five years; the surveys would also benefit from development to add a focus on risk. Liaison with the FIU is good with three meetings being held between the two bodies in 2017. Officers of the Chamber have received training from the FIU and, as lawyers, they have participated in seminars for that profession.

385. The Bar Association has some twenty employees although none is assigned to AML/CFT. Notwithstanding this, the equivalent time of one person is devoted to matters directly or indirectly linked to AML/CFT. AML/CFT forms part of the curriculum for the Bar exams; the Association does not yet undertake AML/CFT supervision.

Table 22: Number of AML/CFT on-site inspections conducted to DNFBPs by DNFBP supervisory authorities

Year	FIU*	GCA	LAO	Chamber of Notaries	Lithuanian Bar Association
2013	7 to company service providers; 4 to casinos	4 to casinos	722 to DPMS	N/A	N/A
2014	1 to a real estate agent; 14 to casinos; 2 to company service providers	14 to casinos	624 to DPMS	4 to notaries	N/A
2015	7 to real estate agents; 14 to casinos; 3 to company service providers; 5 to car dealers	19 to casinos	516 to DPMS	5 to notaries	N/A
2016	2 to real estate agents; 2 to company service providers; 9 to car dealers	14 to casinos	443 to DPMS	0	N/A
2017	2 to real estate agents; 7 to car dealers; 4 joint inspections to casinos	9 to casinos	414 to DPMS	5 to notaries	N/A
Total	79	43	2719	14	N/A

* The table does not include joint FIU on-site inspections to FIs.

Remedial actions and effective, proportionate, and dissuasive sanctions

386. The effectiveness of use of sanctions for the framework as a whole has been reduced to some

extent by gaps in the legal framework and cannot be considered to be wholly dissuasive for the period under review. Recent legislative amendments have been made to address these gaps. While, overall, the number and level of sanctions has not been high in the period under review, there was an improvement in 2017. Additional staff resources will be beneficial in ensuring a fully dissuasive framework.

BOL

387. The BoL requires remediation of breaches and this is monitored by requiring the FI to provide an action plan, a meeting to discuss the action plan and the provision of information demonstrating how the plan is being met. Remedial actions are followed up at the next onsite inspection.

388. As indicated by the table below, the BoL has the will to impose sanctions. Internal guidance has been developed on which sanction should be selected and for calculating the level of a fine. The BoL has the ability to use the sanctions in the AML/CFT Law as well as a palette of sanctions under banking legislation for AML/CFT breaches – it considers that, during the period under review, it has not been able to impose a strong sanction on only one occasion. In the single case in question, it considers the warning imposed on a particular entity to have been effective as it led to a change of management. Warnings are generally issued with a mandatory instruction to remedy breaches within a specified time frame.

Table 23: Sanctions imposed on FIs by the BoL

Type of FI	2012	2013	2014	2015	2016	2017
Banks	1 written warning including publication on the BoL website	2 written warnings including publication on the BoL website	0	0	Information in relation to the onsite inspections of 2 foreign bank branches was published on the BoL website	1 fine of EUR 235,350 and a requirement for the bank to eliminate the deficiencies, including temporarily lending restriction and publication on the BoL website
Credit unions	1 withdrawal of license, including publication on the BoL website	1 removal of manager/compliance officer, including publication on the BoL website	1 written warning, including publication on the BoL website; 1 limitation of activities due to manager's reputation	1 moratorium (suspension of activities), including publication on the BoL website	0	3 written warnings and 1 moratorium, including publication on the BoL website

Financial Brokerage Companies (incl. branches)	0	1 fine of 50,000 Litas (~EUR 14,480), including publication on the BoL website	1 withdrawal of licence, including publication on the BoL website	2 written warnings, including publication on the BoL website	0	0
Life insurance companies (incl. branches)	0	0	1 fine of EUR 28,962 including publication on the BoL website	1 fine of EUR 11,674 and 1 sanction taken to court, including publication on the BoL website	0	1 written warning and publication on the BoL website
Payment institutions	0	0	0	1 fine of EUR 19,731 for failing to provide information on change of manager; 1 written warning for failing to provide information on change of manager; 1 suspension of voting rights of shareholder due to not meeting the reputation requirements; all sanctions published on the BoL website	5 written warnings and 1 fine for failing to provide information on change of manager; all sanctions were published on the BoL website	0
EMIs	0	0	1 written warning, including publication on the BoL website	1 fine of EUR 11,674 including publicising on the BoL website	1 written warning, including publication on the BoL website	1 written warning, including publication on the BoL website

389. The range of penalties used includes warnings, fines, suspension of activities, publication of penalties and, in one case, removal of a manager/compliance officer. Sanctions have been applied as a result of failures to provide information on controllers promptly and as a result of onsite inspections.

The range of sanctions available for non-bank FIs was less strong than that for banks until the summer of 2017. The BoL sees this issue as successfully mitigated for two linked reasons. First, it focusses significant supervisory efforts on banks which have by far the highest materiality and ML/FT risks and there are only two non-banks which are considered to be high risk. Second, these two non-bank institutions were placed under enhanced monitoring, including inspections, and both were subject to penalties. Inspections of other FIs indicated non-significant breaches for which the sanctioning regime was considered to be adequate.

390. The main breaches identified during on-site inspections have been deficiencies related to the quality of risk assessments, and comprehensiveness of CDD and monitoring procedures. The evaluation team accepts that, subject to the one exception identified above, the level of sanctions applied by the BoL has been commensurate with its supervisory findings. There are very good elements of effectiveness and dissuasiveness in the range of sanctions imposed and the routine publication of sanctions but the evaluation team considers that, for the regime to be fully effective and dissuasive, a greater volume of supervision would need to be undertaken than that of the period under review (while noting the significant increase in onsite inspections from 2017).

DNFBP supervisors

391. The GCA provides feedback to casinos after an inspection. A deadline is set to remediate any breaches and the casino is required to inform the GCA routinely of progress. An inspection is undertaken after the deadline has passed.

392. The GCA has been able to impose administrative penalties on legal persons and individuals for AML/CFT breaches since the summer of 2017. Its experience is that there are no systemic AML/CFT failures within the casino sector. It has not imposed any administrative penalties but in 2017 creatively suggested that the FCIS should undertake several onsite inspections so that, if necessary, the FIU could use its wider powers of sanction. Four e-casinos were inspected by the FIU at the request of the GCA (all four received fines of EUR 550 or 2,100 from the court).

393. Early in 2018 the GCA applied to the court for the imposition of a fine of EUR 1,600 against a casino as a result of inadequate CDD for a client; the penalty was agreed by the court and imposed (the court's decision was upheld on appeal after the onsite element of the evaluation).

394. Where AML/CFT breaches are not significant, the FIU requires an inspected firm to remediate the issues within seven days. The more significant breaches result in sanctions (although there is no corresponding written requirement to remediate the failings). Until the summer of 2017, the court rather than the FIU had the ability to impose fines. Therefore, when the FIU wished to impose fines it made an application to the court, including in respect of the sanctions arising from the inspections undertaken at the request of the GCA. The court has routinely made decisions to impose fines but at such low levels that the FIU has challenged them. It has usually won the appeals and, over time, the level of financial penalties has increased. The FIU allowed a grace period of one year after the coming into force of the 2017 AML/CFT Law before making any applications for fines to be levied. The level of cooperation by the DNFBP is a significant factor in deciding whether to move forward a penalty. It considers the powers of sanction are now sufficient.

395. All accountants inspected had breaches of AML/CFT obligations, which has led the FIU to seek the imposition of a fine by the court in every case. It did not appear that the penalties had been imposed by the time of the evaluation team's visit to Lithuania.

396. The Chamber of Notaries' Court of Honour has applied sanctions for shortcomings by notaries

on grounds of reputation and character. These are: 2013: two censures and one disciplinary proceeding; 2014: requiring one notary to make a public apology; two reprimands; one strict reprimand and, one disciplinary proceeding; 2015: two disciplinary proceedings and one censure; 2016, suspension of a notary from professional activities for three months followed by removal by the Minister of Justice of the notary from office; 2017: a decision to make a recommendation to the Minister of Justice to remove a notary from office (approved in June 2018).

397. In 2016 the Bar Association imposed one decision to remove a person from the list of advocates' assistants, one public reprimand, four reprimands, and 12 remarks (i.e. a decision placed in the record of the individual); there were also 13 decisions not to impose a penalty after a case hearing and 6 decisions to terminate disciplinary proceedings. In 2017 there were 12 decisions to delist advocates, 3 decisions to remove individuals from the list of advocates' assistants, 3 public reprimands, 7 reprimands, and 13 remarks; there were also 22 decisions not to impose a penalty after a case hearing and 7 decisions to terminate disciplinary proceedings. While these sanctions have not involved AML/CFT matters they have involved shortfalls in high moral character and demonstrate a broad willingness to impose sanctions. The proportion of cases where sanctions were not applied is considered by the Bar Association to be appropriate, noting that disciplinary actions against advocates are heard by the Court of Honour of Advocates under a procedure established by the Bar Association. Disciplinary sanctions are considered by the Association to be extreme measures and applied only after careful and thorough examination, which is done by three different bodies of the Association. The evaluation team considers there would be merit in the Bar examining its sanctions framework.

398. No sanctions have been applied by the LAO; the assessment team has a concern that this represents a shortfall in the supervisory process and/or the willingness to apply sanctions and/or a lack of processes to do so.

Impact of supervisory actions on compliance

399. Most supervisory authorities, most notably the BoL, were able to point to improvements in AML/CFT compliance as a result of their interventions.

400. The BoL has seen a significant improvement in compliance since 2013 as a result of its efforts. Responses to the questionnaires have improved markedly. FIs have increased the number of staff engaged in AML/CFT. The BoL's AML/CFT inspections of, and outreach to, banks and non-banks have had a marked effect (e.g. increases in STRs submitted by banks). Its supervisory approach has been to require effective CDD to be undertaken by FIs so that they can monitor relationships and transactions adequately, and improvements in both have been noticeable. The BoL has also noted increased understanding of risk by banks. FIs made positive comments to the assessment team about the improvement in the BoL's approach during the last two years. The BoL is also conscious that its limited resources until recently have meant that it has had to focus its overall efforts thematically (principally in relation to licensing and cash transactions), and that this has been at the expense of other aspects of supervision and, therefore, increased effectiveness of compliance by FIs. Future plans include the issue later in 2018 of FAQs with examples of good and poor practices and guidance

on CDD[69].

401. The GCA has noted that compliance by casinos has improved since the summer of 2017 as a result of its inspections, outreach and consultation with the sector on its offsite questionnaire. This increased compliance is underpinned by greater knowledge and awareness of AML/CFT issues since the amendments to the AML/CFT Law came into force, together with better internal policies and procedures.

402. The FIU considered that its inspection programme is well known to the sectors it supervises and that this has increased AML/CFT standards, including in particular increased STR and CTR reporting by notaries. It has also noted a tangible improvement in compliance by inspected entities through the appointment of additional staff and enhanced STR reporting.

403. The Chamber of Notaries advised that an increase in the number of STRs made by notaries in 2017 demonstrates an improvement in compliance.

404. The Bar Association has noted improvements to the quality of consideration of compliance by advocates since the recent revision of the Bar Law. This view derives in large part from additional requests for information and training on AML/CFT. The Bar Association has also noted that advocates who are more recently qualified have a better understanding of the importance of AML/CFT. The Association advised the assessment team that it will take some time for the advocacy provision as a whole to come to terms with a move of emphasis from client privilege to an understanding of the importance of, and compliance with, the AML/CFT framework. This will affect the level of reporting of suspicion.

405. The LAO has noted an increase in the number of AML/CFT questions posed by dealers and suggested that this was indicative of an improvement in compliance.

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

406. The BoL and most DNFBP supervisory authorities have endeavoured to promote understanding by supervised entities of their obligations and risks. Discussions (both at the individual institutional and group level) have been held with FIs. The BoL provides annual training for each sector, as well as meeting regularly with FIs (annual compliance meetings) and provides guidance at those meetings on how to interpret AML/CFT requirements. As with other areas of supervisory engagement, additional staff resources are needed so that further guidance can be introduced and outreach can be undertaken in a systematic way; this will also address the lack of practical examples and typologies noted by supervised entities.

407. The BoL has been particularly active in light of its level of staff resources; it has a more open relationship with FIs than was previously the case. Nevertheless, FIs noted that more guidance is needed. The assessment team agrees with this and notes that the provision of systematic outreach requires some additional staff resource. The provision of training on areas such as risk assessment and the distinction between ML and FT risks and the issue of more comprehensive guidance (indicating good bad practice) is planned by the BoL, including by proactively asking FIs for issues which would benefit from clarification.

[69] After the on-site visit the BOL posted frequently asked questions and responses on its web site and published some guidance for the financial market, which can be found https://www.lb.lt/en/faq-prevention-of-money-laundering-and-terrorist-financing

408. The BoL has devoted significant resource to the new-comers programme and provides information via licensing and supervisory processes. In addition, it answers queries made by FIs. The BoL meets banks as a group annually to discuss both general and topical issues. It endeavours to provide outreach to different types of FI and to focus on sectors and their products rather than on general training. As part of this, the BoL also invites the FIU to join it on some training events. Onsite inspections tend to lead to enhanced contact with FIs for several months, which in turn improves compliance.

409. The GCA has consulted on AML/CFT matters and regularly responds to queries and gives advice to casinos. The GCA made training a focus from 2016 and it has encouraged all casinos to participate in training. In practice, there has been a high level of attendance for the high level training provided to casinos by the GCA (on practical matters) and the FIU (on suspicion) in each of 2016 and 2017. Inspections, the AML/CFT questions in the general questionnaires circulated before 2018 and the detailed AML/CFT-specific questionnaire issued in 2018 are also considered to be part of the GCA's outreach and an aid to promoting understanding of risk.

410. The FIU has been proactive both in relation to DNFBPs it supervises and in working with the other authorities, and its input was noted positively by firms met by the assessment team. Each year it has worked with the BoL to provide training to DNFBPs. In addition to placing AML/CFT information on its website, the FIU also deals with a considerable number of enquiries for information or guidance by DNFBPs.

411. The Chamber of Notaries responds to queries made by notaries on a daily basis and it has placed information on its website (FAQs and recommendations). Together with the FIU, it has sponsored an AML/CFT event for notaries in 2017. It was mindful that training could be improved.

412. The Bar Association's website does not cover AML/CFT but it has organised two seminars which have included AML/CFT has part of the subject matter.

413. The LAO has placed AML/CFT information on its website, including the NRA, as well as news of training events hosted by the FIU for dealers. One event was held in 2017.

Conclusion

414. **Lithuania has achieved a moderate level of effectiveness for IO.3.**

CHAPTER 7. LEGAL PERSONS AND ARRANGEMENTS

Key Findings and Recommended Actions

Key Findings

1. The Centre of Registers published guidance on its website (in Lithuanian and in English) on the manner in which legal persons are created in Lithuania, as well as information on the different types, forms and basic features of legal persons.

2. While Lithuania has not conducted a formal assessment of risks posed by legal persons, it is universally understood by competent authorities that the use of fictitious private limited companies in criminal schemes constitutes a significant ML/FT risk.

3. The Register of Legal Entities ("RLE") maintains basic information on all types of legal persons, which is publicly-available. This ensures that access to competent authorities is timely. However, there is no system to ensure that the information is kept accurate and current.

4. Shareholder[70] information on the vast majority of legal persons is available either from the RLE or at the Information System of Members of legal Entities ("JADIS"), which jointly hold information on 83.8% of legal persons registered in Lithuania. Shareholder information in JADIS is available to competent authorities (free of charge) and to reporting entities (against a fee), though this information is not verified to ensure that it is accurate and current.

5. The mechanism to ensure availability of BO information relies on CDD performed by private sector entities, mainly banks, which verify information on the basis of information maintained at the RLE and JADIS. Given that most legal persons registered in Lithuania are owned and controlled by Lithuanian natural (81.1%) and legal persons (6.6%), this mechanism is broadly adequate with respect to legal persons whose information is contained in JADIS. In fact, competent authorities have not encountered any difficulties in obtaining BO information in this manner. However, there remains a small gap with respect to some legal persons in relation to which information is not available at the RLE or JADIS (16.2% of all legal persons). Additionally, there is no system of verification of information entered into JADIS. Furthermore, there is no complete information on the number of Lithuanian corporate shareholders whose shareholders are legal persons registered outside of Lithuania.

6. Lithuania has implemented effective mitigating measures against the use of fictitious private limited liability companies for criminal purposes, which are considered to pose highest risk, compared to other legal persons. The STI actively monitors information on VAT payers to identify fictitious companies. Many cases involving the use of fictitious companies have been prosecuted. The FIU conducts typology exercised to assist in determining the scale of the problem and forward cases to LEAs.

7. Despite the fact that the Code of Administrative Offences foresees sanctions in case of failure to meet the requirements for timely submission or submission of incorrect information to the RLE/JADIS, no sanctions have been applied in practice. There have been nine instances where fictitious companies have been liquidated.

8. Bearer shares are prohibited in Lithuania. The fact that CSPs are not registered creates a gap in the transparency of legal persons. No mechanism is in place requiring the nominee shareholders and directors to disclose their identity to the relevant register and to make this information available to the competent authorities upon request.

Recommended Actions

Lithuania should:

1. conduct a comprehensive assessment of ML/TF risks in relation to all types of legal persons, including typologies such as use of fictitious companies.

2. expand the record of information on shareholders in the RLE or in JADIS in order to include all types and forms of legal persons created in the country.

[70] The term "shareholder" is used across this chapter but should also be understood as "member", "owner" or "participant" depending on the form of legal person.

3. introduce a mechanism to ensure that information submitted to the RLE and JADIS is adequate, accurate and up-to-date.

4. apply dissuasive and proportionate sanctions against legal entities for failure to comply with the requirements on submission of basic information.

5. address technical shortcomings in relation to R. 24.

415. The relevant Immediate Outcome considered and assessed in this chapter is IO5. The recommendations relevant for the assessment of effectiveness under this section are R24 & 25[71].

Immediate Outcome 5 (Legal Persons and Arrangements)

416. By way of context and materiality, it should be noted that Lithuania is not a company formation centre. No specific benefits (e.g. reduced corporate tax rates or exemptions) are offered to non-residents wishing to set up companies in Lithuania for use in international business. The authorities advised that it is not common for Lithuanian companies to be set up as part of complex corporate structures (e.g. as a holding company). Lithuanian legislation does not provide for the creation of legal arrangements, such as trusts.

417. As at the end of 2017, there was a total of 224,027 registered legal persons[72] in 30 different legal forms. The following five legal forms represented almost 90% of the total: private companies limited by shares (124,122), individual enterprises (37,270), associations (18,948), small communities (11,897) and public institutions (10,554). Companies in Lithuania, consisting of private companies limited by shares and public limited liability companies, represent around 56% of the total.

418. 87.7% of the total number of shareholders are Lithuanians: 81.1% are natural persons; 6.6% are legal persons. 12.3% are non-resident shareholders: 9.8% are natural persons and only 2.5% are legal persons, mainly from Estonia, Latvia and the UK.

419. Private limited liability companies are by far the most common form of legal persons involved in ML and criminal schemes, based on statistics and data gathered from LEAs and supervisory authorities.

Public availability of information on the creation and types of legal persons and arrangements

420. The Civil Code regulates the manner in which legal persons may be created and stipulates the different types and basic features of legal persons. The Centre of Registers published guidance on its website[73] (in Lithuanian and in English) on the manner in which legal persons are created in Lithuania, as well as information on the different types, forms and basic features of legal persons.

421. The incorporation of a legal person in Lithuania is generally considered to be a straightforward process. The registration of the most common types of legal persons (private limited companies,

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

[72] and 4,370 branches or representation offices of legal persons

[73] http://www.registrucentras.lt/en/ (under the tab "Legal Entities")

associations, small communities, public institutions, charities and relief foundations) can be made online without the intervention of a notary through an electronic service introduced in 2010 by the Centre of Registers. It takes one working day to complete the registration process. The authorities have advised that 70 per cent of legal entities are registered electronically. The service, available for citizens of Lithuania only, requires no paper documents and relies on the use of an electronic signature. In the case of legal entities not registered electronically and in the case of non-resident founders the service of a notary to form a legal person is required. An e-Guide for starting business in Lithuania is currently provided for non-resident persons to assist them in incorporating and registering companies.

422. The RLE pursues a policy of transparency in relation to Lithuanian businesses, institutions and NGOs by maintaining complete information (and historical data) about legal form and status of legal entities, nature of their activity, size and structure of the authorised capital, licenses acquired, etc. Information such as name, code, registered address, legal form, legal status is publicly-accessible free of charge, annual financial statements or copy of any other document (such as memorandum or articles of association or board minutes) stored in the RLE may be provided for a fee set by the Government.

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

423. Lithuania has not conducted a formal assessment of the ML/FT risks posed by different types and features of legal persons that may be incorporated in Lithuania. The NRA simply highlights the risks around inadequate verification of BO information by DNFBPs where they are unable to identify the BO of complex structures and failure by FIs to verify a foreign BO of a Lithuanian legal person with chain ownership. These conclusions are based on hypothetical scenarios referring to well-known international typologies rather than cases identified domestically. As already mentioned in the introduction, the involvement of Lithuanian legal persons in international complex structures is limited.

424. While the country has not gone through the motions of identifying and assessing the risks posed by the totality of legal persons, there is universal understanding among competent authorities that the use of fictitious companies, taking the form of private limited companies, poses a significant risk both in terms of ML and for wider criminal purposes. The understanding of the authorities is based on cases encountered through their operational activities, particularly as far as the STI, the FIU and LEAs are concerned. A fictitious company is understood by the authorities to be a shell company set up for the purposes of conducting fictitious transactions or entering into fictitious agreements to conceal criminal activity or evade taxes. The structure is generally simple and its shareholders and directors are either the persons controlling the criminal scheme themselves or front persons. It does not appear that these are set up through CSPs. Mitigating measures are being taken, as explained under core issue 5.3, to thwart this activity and reduce the scale of the problem. Despite these efforts, the scale of this phenomenon is not known with certainty, in the absence of a more scientific assessment. For instance, there are indications that fictitious companies are also misused by non-residents. The extent to which this happens is not known, although it is to be noted that only 12.3% of shareholders of Lithuanian legal persons are non-resident.

425. It is not clear whether the private sector has been informed of the various techniques criminals can employ to launder the proceeds of their illicit activity through fictitious companies. Despite of

this, banks demonstrated a good understanding of the risks related to fictitious companies and take mitigating measures as indicated under IO 4.

426. One of the areas of increased focus of this report refers to non-resident business and the extent to which Lithuania has considered whether Lithuanian legal persons form part of complex corporate structures involving legal entities or arrangements. As mentioned in chapter 1, following the Panama Papers leaks, the BoL conducted a study in 2016 to gauge the extent to which the banking sector (and the largest e-money institution) services customers from IFCs. It was concluded that the exposure was limited and, as a result, the risk arising from non-resident business was assessed to be low. This was further confirmed by the assessment team on the basis of additional information (including on the volume, origin and destination of wire transfers) and analysis of statistics provided by the authorities, particularly the RLE. However, Lithuania does not appear to maintain complete information on the number of customers that are legal persons registered in Lithuania which are beneficially owned by non-residents, although this does not appear to constitute a major issue.

Mitigating measures to prevent the misuse of legal persons and arrangements

Measures relating to basic information and information on shareholders

427. The RLE holds basic information on all types of legal persons. This information is publicly-accessible on-line. Shareholder information is maintained and made public on-line by the RLE with respect to single shareholder companies, state-owned enterprises, municipal enterprises, budget institutions, true partnerships, partnerships, individual enterprises, households, lawyers unions. Shareholder information of other forms of legal persons is available through another (parallel) online platform, the Legal Entities Information System (JADIS). JADIS contains shareholder information on private limited liability companies, public institutions and small communities. Information on shareholders available in the RLE and JADIS represents 83.8% of the total amount of registered legal persons. The scope of the legal persons included in JADIS will broaden in the near future as it is already foreseen to include five additional types of legal persons[74]. There are no concrete plans yet to incorporate information on the remaining types of legal persons within the system.

Measures relating to beneficial ownership information

428. At the time of the on-site visit, the mechanism in place to ensure the availability of BO information relied on CDD performed by the private sector, mainly banks. Customers that are legal persons are requested to provide BO information, which is then verified by checking information held at either the RLE or JADIS, where data is easily accessible. The process is relatively straightforward where the shareholders of the legal person are natural persons (91% of the cases). Banks indicated that where shareholders (or directors) who are natural persons appear to act as front persons, this would likely indicate the existence of a fictitious company and raise suspicion, prompting the submission of an STR to the FIU. As noted under IO 7, such cases have been identified (see for instance Box 7.1). Where the shareholders of the legal persons are themselves companies (corporate shareholders), in most cases, information on the natural persons owning or controlling those corporate shareholders may be found in JADIS, as most corporate shareholders are registered in Lithuania (6.6% of 9% of total corporate shareholders). As noted in the introduction, only 12.3% are non-resident shareholders: 9.8% are natural persons, mainly from Ukraine, the Russian Federation,

[74] Cooperatives and Agricultural Companies in November 2018, Partnerships and True Partnerships in January 2019, Charity foundations at a later stage.

Belarus and Latvia and only 2.5% are legal persons, mainly from Estonia, Latvia and the UK (owned by Lithuanians residing there). In these cases, private sector entities request the legal person to provide extracts from foreign registries for verification purposes. While this mechanism functions adequately with respect to legal persons whose information is registered in the RLE or JADIS, there remains a small gap with respect to other legal persons. Additionally, there is no system of verification of information entered into JADIS. Furthermore, there is no complete information on the number of Lithuanian corporate shareholders whose shareholders are legal persons registered outside of Lithuania. As a final point, although shortcomings were identified with respect to the verification of BO by the private sector under IO 4, the assessment team wishes to emphasise that these relate to customers that are legal persons registered outside of Lithuania and are, therefore, not relevant to IO 5.

429. At the time of the on-site visit, provisions were in place within the AML/CFT Law requiring legal persons to receive, update and store detailed information about their BOs and submit this information to JADIS. However, this requirement will only enter into force on 1 January 2019 and the specified information on the BOs must be submitted to JADIS by no later than 1 July 2019[75].

430. Turning to fictitious private limited companies, which appear to pose the highest ML/FT risk, the STI actively monitors tax payers to identify those which do not undertake any economic activities. The STI has the power of removing such tax payers from the register of VAT payers. Various indicators have been identified[76] by the STI in order to expose infringements. In the period under review, 21,914 companies were removed from the list of VAT payers[77], thus eliminating any possibilities to carry out fictitious economic activity. The STI co-operates very closely with the FCIS to identify fictitious companies. A risk analysis centre, including representatives from both authorities, was set up for this purpose, which as of recently includes the participation of the Prosecution Service. The purpose of the centre is to analyse information with a view to identifying violations in the area of taxes and crimes against the financial system and preventing and investigation such crimes. As a result, in 2013-2017, the Prosecution Service prosecuted 222 legal persons in criminal proceedings and handed criminal cases with 159 defendant legal persons over to the court for examination. The large majority of these cases related to fictitious companies. Investigations in respect of 63 suspected companies were terminated. Liquidation has been the most common criminal sanction imposed on fictitious companies. There are currently ongoing criminal proceedings against 29 fictitious companies. The FIU periodically conducts a typology study based on STRs which identifies the use of fictitious companies in criminal schemes. For instance, in 2017, the FIU identified 22 cases related to activities of allegedly fictitious companies engaged in a wide range of activities, such as international freight, construction, consultancy, repair of vehicles, etc. Information was disseminated to LEAs, which initiated various investigations and brought charges, including for ML, against the persons controlling the criminal schemes and the companies themselves. These cases are still on-going. A number of proposals were made by the GPO to the Minister of Justice to strengthen the fight against the use of fictitious companies. These proposals include, for instance, the imposition of stricter

[75] This has not been considered for conclusions or rating as it was not in force and effect at the time of the on-site visit.

[76] The company is not found at the official registered address; does not present VAT declarations or declares repayable VAT only; does not present financial accountability documents; does hire employees; fails to fulfil the instructions by the STI; does not carry out any real economic transactions but documents them in accounting books; the VAT payer is established or incorporated on the basis of forged documents; there is contradicting information on trade with foreign entities; the company VAT code payer is used in tax fraud circumstances.

[77] The total number of VAT payers is approximately eighty thousand per year.

conditions on banks when opening accounts for companies which are VAT payers and expanding the list of transactions which must be concluded and approved by a notary or a bailiff. These proposals have not yet been implemented.

Measures to verify basic information

431. There are no mechanisms in place to ensure that the information entered into the RLE and JADIS is accurate and up to date. This obligation lies with the head/managing body of the company. No information is available to the authorities on the number of instances where inaccurate information was identified. Data submitted to JADIS is confirmed by the applicant with an electronic signature, against a qualified certificate issued by the Centre of Registers. Information on shareholders is required to be submitted by no later than five days after registration with the RLE/JADIS and after a change in shareholders.

432. Where the legal person is not created electronically (30% of the cases) or created by a non-resident, the authenticity and compliance of the submitted documents with the relevant legislative requirements are verified by a notary. The notary, which is a public official who may attribute public faith to documents, is required to verify all the information. Due to the fact that the assessment team has not received information on the verification process conducted by notaries, the effectiveness of this mechanism could not be assessed.

Measures relating to bearer shares and nominee directors and shareholders

433. The Law on Companies states that all shares must be registered, therefore shares in bearer form are prohibited. There is also a provision in the Law on Banks which indicates that banks are prohibited from issuing bearer shares.

434. Although Lithuanian law does not provide for the concept of nominees, the authorities have confirmed that the provision of company services, which may also include nominee directors and shareholders, by corporate services providers is known to happen. Although this does not appear to be a widespread practice, this creates a gap in the transparency of legal persons, especially since there is no system of registration for corporate service providers and there is no requirement for nominees to disclose their status to the company registry. There could be a possibility that CSPs assist in the setting up of fictitious companies, although as stated previously LEAs have not encountered such instances.

Timely access to adequate, accurate and current basic and beneficial ownership information on legal persons/arrangements

435. In terms of timely and adequate access, competent authorities may obtain basic information on each type of legal person from the RLE, which maintains all information and makes it publicly-available online. Competent authorities can obtain shareholder information through the RLE and JADIS. Currently, full and free-of-charge access to the information contained in JADIS is provided to the police, prosecutors, other LEAs, the FIU and other state institutions. Private entities, such as banks, credit unions, notaries, bailiffs and attorneys have access to information contained in JADIS against a fee.

436. In terms of accuracy and currency of basic information, as noted previously, there are no mechanisms to verify this type information. The authorities did not highlight any major problems in this area. In relation to shareholders, information is not available either in the RLE or in JADIS in

relation to 16.2% of legal persons[78]. However, these types of legal persons are not known to be involved in criminal schemes. LEAs noted that they have not often sought shareholder information on these types of entities. Still, this constitutes a small gap in the system.

437. Access to information on BO is obtained through private sector entities, mainly from banks. It should be noted that all legal entities are required to open a bank account in Lithuania in order to deposit the initial share-capital before proceeding to registration with the RLE. Thereafter, the authorities pointed out that it would be inconvenient for legal entities not to have at least one bank account in Lithuania, which ensures that BO information on legal entities is available. The FIU and the LEAs advised that, in practice, they have not encountered difficulties in obtaining BO information from banks. It was indicated that BO information from banks is generally found to be adequate, accurate and current and provided promptly, within the stipulated timeframes. For instance, the FIU indicated that it has been able to provide BO information without obstacles to foreign partners in almost 90% of the requests sent and received. However, as noted under core issue 5.3, there are some gaps in relation to the BO information maintained by private sector entities.

Effectiveness, proportionality and dissuasiveness of sanctions

438. According to the Code of Administrative Offences, failure to submit information in a timely manner or submission of incorrect register data, documents and other information to the RLE or to JADIS is subject to a fine ranging from EUR 30 and EUR 1,450[79]. The assessment team does not consider the level of fines to be proportionate and dissuasive. To date, no sanctions have been imposed with regard to the submission of inaccurate basic information or failure to submit such information in a timely manner. This is not surprising since there are no mechanisms in place to verify the accuracy of the data and no authority is responsible for monitoring the information held at the RLE/JADIS. Since July 2017, the Centre of Registers transmitted a total of 405 protocols to the courts which imposed 283 sanctions. 226 of them were fines for a total of EUR 44,200. These numbers include only breaches with regard to the submission of incorrect financial statements.

439. With respect to fictitious companies, if a prosecutor establishes that a company has been established on fictitious grounds, the court may be addressed with a claim requesting the liquidation of that legal person. In 2013-2017, the Prosecution Service addressed 10 cases to the courts, which resulted in the liquidation of 9 companies.

Conclusion

440. **Lithuania has achieved a moderate level of effectiveness for IO5**.

[78] Associations, communities, trade unions or associations, charities and support foundations, gardeners communities, traditional religious communities or societies, agricultural companies, cooperatives, religious communities or societies, permanent commercial arbitration bodies, chambers of commerce, industry and crafts, European economic interest grouping, credit union, European company, association of Lithuanian chambers of commerce, industry and crafts, general management and notification center.
[79] In relation to financial statements, the fine ranges between EUR 200 and EUR 3,000.

CHAPTER 8. INTERNATIONAL COOPERATION

Key Findings and Recommended Actions

Key Findings

1. Lithuania has a sound legal and procedural framework to exchange information and cooperate with its foreign counterparts in relation to ML, associated predicate offences and FT. Information is exchanged comprehensively, proactively and in a timely manner, both upon request and spontaneously. The evaluation team received positive feedback from the AML/CFT global network in relation to the quality and timeliness of assistance provided by Lithuania.

2. Lithuania actively seeks international co-operation from other states. This has resulted in convictions and the seizure and confiscation of proceeds of crime, as evidenced by various case studies provided to the assessment team.

3. Effective cooperation between Lithuania and other EU Member States is well-developed, especially with the other Baltic States. Regular cooperation based on UN instruments and bilateral agreements also takes place outside of the EU, especially with neighbouring countries.

4. On average, requests for MLA are processed within 1 to 4 months, depending on the nature of the request, the type of assistance requested and the complexity of the request. Urgent requests are executed within shorter time-frames.

5. The authorities advised that not a single MLA request related to ML/FT was refused in the period under review. This was also confirmed by the AML/CFT global network. In the few instances where MLA was not provided in relation to predicate offences, the authorities explained that this was due to deficiencies in the form and content of a request as laid down in international treaties, statute of limitations and/or requests relating to acts which did not involve criminal liability.

6. While extradition figures show that only a portion of extradition requests is actually executed, the authorities explained that a significant part of these requests involved persons who did not reside in Lithuania. The others were refused on the grounds that Lithuania cannot extradite its own nationals.

7. MLA requests sought and received usually involve the following: interviewing witnesses, interrogation of suspects, provision of information on ongoing or completed criminal proceedings, provision of copies of documents, freezing of property, collection of evidence, and obtaining information on bank accounts, records, bank statements, information on mobile phone statements.

8. There are two central authorities involved in the processing of MLA requests, the MoJ for judicial requests and the PGO for criminal procedural requests. Both have a case management system in place. While there are no formal prioritisation rules for incoming MLA requests, the MoJ, the PGO and other LEAs follow EU best practices and all requests related to higher risk crimes automatically receive priority. Other factors taken into account when prioritising cases are: the nature of requested actions, the severity of the crime, the complexity of the case and whether the case involves restraint of assets.

9. Although the MoJ and the PGO have a case management system in place, MLA requests are not categorised according to type of offence and therefore clear statistics on requests relating to ML, associated predicate offences, and FT are not available.

10. The FIU has a broad legal basis for the exchange of information with its foreign counterparts. Spontaneous information is regularly exchanged. The assistance provided is considered effective in terms of timeliness and quality.

11. LEAs are also active in the sphere of informal cooperation through direct communication via Europol, Interpol, SIENA and CARIN. The creation of joint investigative teams between Lithuanian LEAs and their foreign counterparts on large scale cases has become increasingly common.

12. The BoL makes full use of a large number of bilateral and multilateral agreements to exchange information with its counterparts, especially in relation to AML/CFT on-site inspections.

13. Exchanges in relation to basic and BO information in relation to Lithuanian legal persons takes place on a regular basis. The feedback provided by the AML/CFT global network does not suggest particular concerns in this respect. However, the weaknesses identified under IO.5 could potentially affect the authorities' ability to exchange BO information.

Recommended Actions

1. Both the MoJ and the PGO should introduce a system to maintain comprehensive statistics on international cooperation, including specific statistics for ML/FT-related cases, the underlying criminality and the time taken to respond to requests.

2. The authorities should apply measures to ensure that the effectiveness of incoming MLA requests is not hindered by the issues concerning BO information (referred to under IO.5).

Immediate Outcome 2 (International Cooperation)

Providing and seeking mutual legal assistance and extradition

441. Lithuania has a sound legal and procedural framework to exchange information and cooperate with its foreign counterparts in relation to ML, associated predicate offences and FT. This has been confirmed through interviews with all relevant competent authorities and case studies provided to the assessment team. Information is exchanged comprehensively, proactively and in a timely manner, both upon request and spontaneously.

442. The Ministry of Justice (MoJ) and the Office of the Prosecutor General (PGO) are the central authorities for the receipt, processing and allocation of mutual legal assistance (MLA) requests. During the pre-trial stage, the competent authority for incoming and outgoing MLAs is the PGO. At the court review stage, the competent authority is the MoJ for both incoming and outgoing MLA requests. Extradition requests are handled solely by the PGO. Where MLA requests are received directly by the courts, prosecutors or pre-trial investigation officers, their execution is subject to authorisation by the MoJ or the PGO

443. MLA, including extradition, is carried out in accordance with the provisions of the CPC and a broad range of international treaties ratified by Lithuania, resolutions of the United Nations Security Council, EU legal acts and bilateral agreements (see Rec. 37-39, TC Annex). In the absence of an international treaty, MLA may be provided on the principle of reciprocity. In this case, MLA request must not contravene the Constitution, national legal acts and the fundamental principles of criminal procedure.

444. The EU legal instruments applicable to Lithuania (including European Investigation Order and European Arrest Warrant) provided a basis for simplified and expedited cooperation with EU member states. Co-operation amongst Lithuania and the other Baltic countries is particularly well-developed. Lithuania also actively co-operates with third countries, especially its neighbouring non-EU countries. The few obstacles that have been encountered in relation to third countries related to differences in legal systems and poor quality translations or preparation of requests, which were solved swiftly through direct communication with the counterparts concerned.

445. MLA requests are sent and received through IT secure channels made available, for instance, through Eurojust, the European Judicial Network (EJN) and the ARO platform. Requests can also be sent by post (privileged and confidential). MLA requests can also be transmitted through diplomatic channels, when so permitted by an international treaty. In urgent cases, requests may be sent via e-mail or fax. In such cases, the assistance of the Lithuanian appointee at Eurojust or his deputy may be used or the contact points at the EJN. Direct communication with foreign partners is sometimes used for prior consultations and/or the co-ordination of operations, thus enabling quicker and more efficient action.

446. All outgoing and incoming MLA requests are registered in the MoJ's document management system. The MLA requests handled by the PGO are registered in the Information system of the Prosecution Service (IPS), which includes statistical information on all requests for legal assistance that are executed. The monitoring of progress of all requests registered in the IPS takes place through the electronic Document Management System (DVS). However, neither the system of the MoJ nor that of the PGO allows for the categorisation of MLA requests per legal qualification (whether it is a civil or criminal request, the type of offence, etc). Therefore, it is not possible to identify the actual number of requests related to ML, associated predicate offences, and FT.

447. While there are no formal prioritisation rules for incoming MLA requests, the MoJ, the PGO and other LEAs follow EU best practices. All requests related to organised criminality, drug trafficking, fraud and other high risk crimes automatically receive priority. Other factors taken into account when prioritising cases are: the nature of requested actions, the severity of the crime, the complexity of the case and whether the case involves restraint of assets. Where the MLA request includes a specific time-frame for its execution, the authorities endeavour to meet the deadlines (e.g. the date of the court hearing is taken into account by the MoJ). Both the authorities and the AML/CFT global network confirmed that urgent requests receive the highest attention.

448. The evaluation team received positive feedback from the AML/CFT global network (feedback was received from 24 states) in relation to the quality and timeliness of assistance provided by Lithuania. On average, requests for MLA are processed within 1 to 4 months, depending on the nature of the request, the type of assistance requested and the complexity of the request. Urgent requests are executed within even shorter time-frames. As far as cooperation with EU countries is concerned, Lithuania adheres to the obligation to execute the European Investigation Order and the European Arrest Warrant within the time-limits indicated in the relevant EU legislation.

449. In line with the PGO's Explanatory Note on Execution of Requests for Legal Assistance from the Authorities of Foreign States, MLA requests in the pre-trial stage are treated within a period of four months. If the execution takes longer, the executing pre-trial investigation officer or prosecutor informs the PGO about the prolongation and planned execution. In such a case, the PGO informs the issuing state about the developments, indicating the reasons thereof. According to the authorities the

cases where prolongation is necessary are rare and are usually based on objective reasons. As a rule, the MoJ monitors the execution of MLA requests solely at the request of foreign counterparts.

450. Lithuania usually requests and is requested to perform the following actions: interview witnesses, interrogate suspects, provide information on ongoing or completed criminal proceedings in respect of a specific person, provide copies of documents, freeze property or collect evidence, and obtain information on bank accounts, records, bank statements, information on mobile phone statements and their subscribers.

451. Lithuania very rarely refuses to provide MLA: 17 requests in 2014, 17 requests in 2015, and 31 requests in 2016. These relate to the total number of MLA requests by both the PGO and the MoJ, relate to requests relating to both criminal and civil matters and should be viewed in light of the figures presented in the tables below. The authorities advised that not a single MLA request related to ML/FT was refused in the period under review. This was also confirmed by the AML/CFT global network. In the few instances where MLA was not provided, the authorities explained that this was due to deficiencies in the form and content of a request as laid down in international treaties, statute of limitations and/or acts which do not relate to criminal liability (e.g. disputes of civil law or administrative offences). The number of MLA letters received by the MoJ in the area of judicial cooperation either in civil or criminal matters is presented in the tables below.

Table 24: MLA requests received by the MoJ

Year	Number of letters
2012	5567
2013	6249
2014	5971
2015	4946
2016	4672

Table 25: MLA requests sent by the MoJ

Year	Number of letters
2012	4560
2013	4859
2014	5220
2015	4200
2016	3964

452. These tables represent aggregated data of incoming and outgoing requests for legal assistance by the MoJ, including repeated requests on civil and criminal matters. Although the current mechanism in place does not allow for the categorisation of MLA requests per legal qualification, the authorities suggest that approximately 25% of the data in the tables relate to criminal matters, 25% to civil matters and 50% to civil registry requests. Therefore, only few of these requests relate to ML/FT offences. The MoJ suggested that MLA exchange is more frequent with neighbouring countries (Belarus, Latvia, Poland, Russia, Ukraine and Estonia).

453. The number of MLA requests received by the PGO is shown in the tables below.

Table 26: MLA requests received by the PGO

Year	Number of requests
2012	655

2013	725
2014	738
2015	855
2016	973

454. It should be noted that all requests made through direct communication between the judicial, the preliminary investigation authorities and Eurojust, which constitute a large portion of the total number of MLA requests, are not reflected in the tables above.

455. Although the Information Data System of the PGO does not allow for the categorisation of MLA requests per legal qualification, the authorities manually categorised all 2017 MLA requests for the purpose of this report. The authorities confirmed that they did not identify any MLA request related to FT, while they identified 12 incoming and 7 outgoing requests related to ML.

Table 27: ML-related MLA requests received by the Prosecutor General's Office in 2017

Country	Number of requests received	Nature of requests	Status
USA	6 (plus a supplementary request)	• Asset freezing;* • copy of the data stored in the server, detailed info about IP the address linked with the server; • detailed info about bank accounts (statements and other related information; Web Money Purse records); • officials' records (business registration, export record, residence permits).	• All requests received were executed on average within a period of three months.
The Netherlands	2	• Identification data of legal persons; • transactions data from Web Purse; • asset freezing.*	
Denmark	2	• Interview of witnesses; • information about bank accounts and their holders.	
Monaco	1		
Liechtenstein	1		

* Asset freezing, in relation to 3 cases, is still ongoing.

Table 28: ML-related MLA requests sent by the Prosecutor General's Office in 2017

Country	Number of requests received	Nature of requests	Status
Belarus	1	• Locate a person and interview him/her as a witness; • provide copies of documents (export records, accounting documents); • carry out searches or seizures; • verify a person with the procedural documents.	• All requests sent were executed on average within a period of four months.
Cyprus	1		
Italy	1		
Liechtenstein	1		
Malta	1		
Poland	1		
The UK	1		

456. Extradition figures show that only a portion of extradition requests is actually executed. The authorities explained that a significant part of the requests received involved persons who did not reside in Lithuania. The others were refused on the grounds that Lithuania cannot extradite its own nationals.

Table 29: Extradition requests received

Year	Number of requests	Executed	Refused	Pending
2014	7	1	2	4
2015	14	6	2	6
2016	11	2	9	0

457. The Lithuanian authorities frequently engage with their foreign counterparts (bilaterally or multilaterally) to avoid or resolve conflicts of jurisdiction as well as to find the most effective and mutually acceptable solutions. They presented examples of a proactive approach in seeking MLA from other states, which resulted in convictions and/or seized and confiscated proceeds. Most of the case studies under IO 7 refer. These case examples reflect several areas of increased risk (in relation to predicate crimes with transnational elements), including drug trafficking and organised crime. As for incoming requests, successful cases of international cooperation have been presented, including cases involving virtual currencies (with the Netherlands and USA) which resulted in freezing of funds.

Box 2.1

Outgoing MLA request (Belarus national)

Based on information received from a Lithuanian bank related to a suspicious financial operation (possible ML), a pre-trial investigation was commenced by the FCIS against a Belarus national, who had the status of a permanent resident of Lithuania and a MLA request was sent to the Belarusian authorities. The Belarus national, holder of a bank account in the said Lithuanian bank, received deposits of approximately USD 1.5 mln from various countries in a period of several years although he did not perform any transaction.

In response to the MLA request, the Lithuanian authorities received information that the Republic of Belarus was conducting a parallel criminal investigation against said person in relation to legalisation of the proceeds of crime, allegedly obtained by means of illegal pharmacy activities. A MLA request followed, by the Belarusian authorities, requesting for assistance in conducting hand-writing expertise. As a result of the assistance provided by the Lithuanian authorities, it was established that the Belarus national had signed the review documents proving his guilt. The person in concern was sentenced in Belarus for tax avoidance and fees on a very large scale.

In the meantime, MLA requests were sent by the Prosecutor General's Office to China, the Special Administrative Region of Hong Kong, and Belarus. The MLA process was initiated by the FCIS, while the PGO was responsible for the coordination and monitoring of during the whole process. The MLA request requested the following:

a) information about the criminal investigations going on in specific countries;

b) copies of the procedural decisions on the outgoing investigations;

c) to serve in witnesses' summons;

d) statements of bank accounts;

e) information on the existence of specific companies; to provide the copies of the documents on the establishment; and

f) to interview the witness, to perform a parade

Belarus executed in 3 months, China in 10 months; and Hong Kong in 2 years. The Lithuanian authorities consider the results satisfactory, although no evidence was found that the funds were obtained from criminal activities. As a result, the pre-trial investigation in terms of ML was terminated.

Box 2.2 – Incoming MLA requests (Cash couriers)

During a criminal investigation conducted by UK LEAs, a number of Lithuanian nationals were found to be involved in a ML case. During a check performed on a vehicle with Lithuanian passengers a large quantity of cash was found– about GBP 150,000. The Lithuanian nationals could not explain the origin of these funds. In June 2013, a MLA request was sent by the UK competent authorities to the Prosecutor General's Office requesting the following actions:

- to establish the origin of these funds;
- to identify the owners of specific mobile numbers and provide statements of telephone conversations during the specific period;
- to provide bank statements on specific accounts;
- to provide data available in national databases related to these persons;
- to interview the witnesses;
- to provide records on previous convictions and etc.

All requested actions were performed and assistance was provided to a full extent, in a period of two and a half months.

Box 2.3 – Incoming MLA requests (Virtual currencies)

Lithuania is currently executing two MLA requests involving the seizure of virtual funds. The first case is related to multiple MLA requests sent in the period between April and June 2017 by the Netherlands, while the second case to a MLA request sent in June 2017 by the United States of America. Both MLA requests were received by the PGO.

It is worthy to note that, prior to the official requests, the national police of the Netherlands had liaised with its Lithuanian counterparts (i. e. the Lithuanian Criminal Police Bureau). The Lithuanian Criminal Police Bureau was responsible for the execution of the MLA requests. On the basis of the last MLA request, received in mid-June 2017, all IT infrastructure of the dark market hosted in Lithuanian passed over to the Dutch national police for further investigation.

As regards the MLA request sent by the US the same coordination process took place between the US authorities and the competent unit of the Lithuanian Criminal Police Bureau. The execution of the request was conducted jointly by the US LEAs and the Lithuanian Criminal Police Bureau. During the MLA execution, crypto currencies (BTC, Monero and Ethereum) of the dark market stored on Lithuanian servers, were seized. New crypto currency accounts (wallets and addresses) had been created prior to the start of the MLA execution. The transfer of funds had been conducted through multiple transactions due to transaction limits (maximum transferrable amount).

In both cases, after extensive consultations (including a coordination meeting) with the PGO, the FCIS and the requesting countries, the seizure of virtual funds was carried out by creating a purse, wherein the virtual money is held. Longer, more cost-effective procedures for seizure were followed by the Lithuanian authorities and their foreign counterparts, due to high transaction fees.

Seeking and providing other forms of international cooperation for AML/CFT purposes

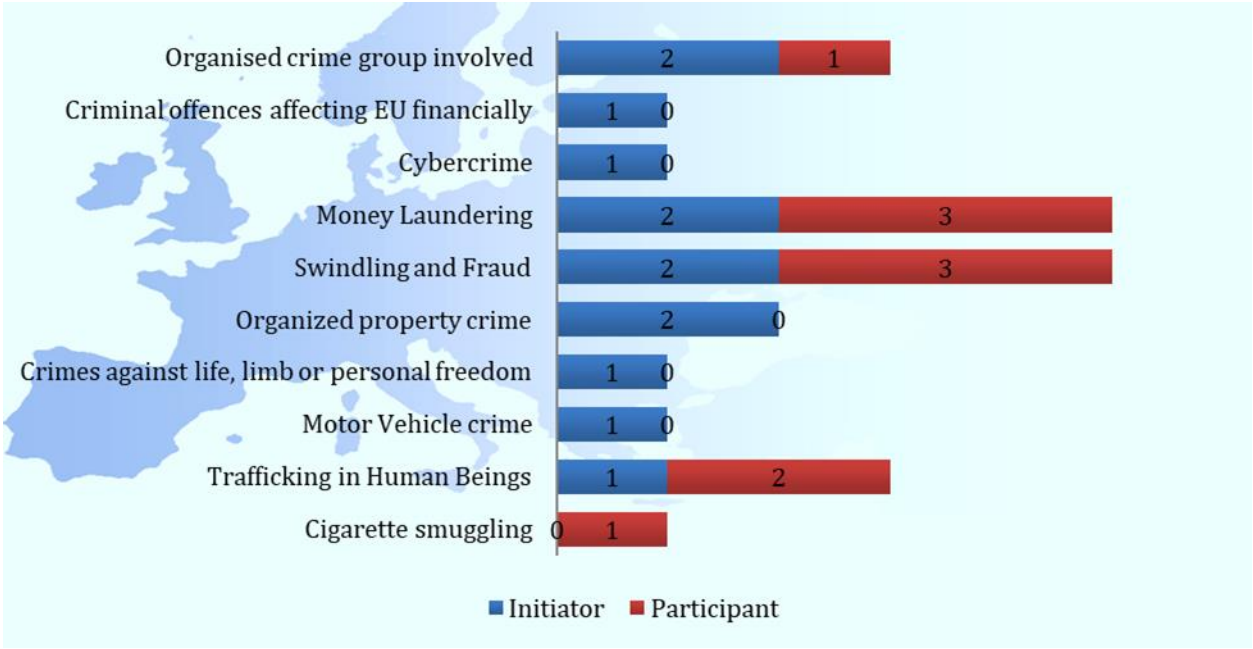
Law enforcement:

458. LEAs frequently use the Secure Information Exchange Network Application (SIENA), Camden Asset Recovery Inter-agency Network (CARIN), OLAF Anti-Fraud Communicators' Network (OAFCN), other networks and direct communication to facilitate and enhance international co-operation.

459. The PGO employs various forms of cooperation such as ad hoc Joint Investigation Teams (JITs), liaison officers (see R.40), special investigative measures (e.g. undercover agents, covert operations, interception of electronic communications including digital and computer communications), tele-video conferencing or coordination meetings, which have proved to be constructive and cost-effective. Assistance from Eurojust, the EJN, the EJTN, European contact points and other networks is used by the Lithuanian authorities.

460. In addition, JITs are established by the Lithuanian investigators and prosecutors while investigating ML cases and recovering proceeds of crime. Lithuania has signed six JIT agreements, four in 2017 and two in 2016, while it provided support under seven other JIT agreements signed in previous years. The most common types of crime investigated by JITs are ML, swindling and fraud. Case-studies under IO 7 refer to a number of investigations which involved the creation of JITs.

461. The chart below illustrates the type of crimes under investigation under the JIT agreements signed by Lithuania.



ARO:

462. The Lithuanian asset recovery office (ARO) in 2017 sent 167 messages and received 213 messages. Additionally, Lithuania sent 32 requests under the conditions laid down in Framework Decision 2006/960/JHA2 ("the Swedish Initiative") out of which 20 related to swindling and fraud, nine related to motor vehicle crime and nine ML-related requests (with a predicate offence: six related to swindling and fraud, two related to drug trafficking, and one related to trafficking in human beings).

Table 30: Requests made and received by the ARO

Year	Requests received from ARO:	Requests sent to ARO:	Requests received from CARIN:	Requests sent to CARIN:	Other type of message sent:	Other type of message received:
2015	33	51				
2016	42	19	14	11	15	19
2017	74	13	8	8	19	17

Table 31: Requests and answers made and received by the ARO within the Swedish initiative on Asset Tracing

Year		Received by Lithuanian ARO:	Sent by Lithuanian ARO:
2016	Answer Swedish initiative (assets tracing)	18	16
	Request Swedish initiative (assets tracing)	14	10
2017	Answer Swedish initiative (assets tracing)	47	35
	Request Swedish initiative (assets tracing)	27	32

FIU:

463. The Lithuanian FIU maintains good co-operation with foreign counterparts, exchanging information comprehensively, proactively and in a timely manner, both upon request and spontaneously. The FIU cooperates not only with its foreign counterparts, but also with non-counterpart authorities within the framework of diagonal cooperation. For the purpose of international exchange of information, the FIU may request information from any RE. However, the authorities confirmed that diagonal co-operation has never been used.

Table 32: STR-related information requests received by the Lithuanian FIU

Year	Number of requests for information
2016	175
2017	193

Table 33: STR-related information requests sent by the Lithuanian FIU

Year	Number of requests for information
2016	318
2017	368

464. The majority of requests received were from Latvia (28), the UK (28), Estonia (11), Moldova (10), the Russian Federation (9), the Netherlands (9), Ukraine (8), Belarus (7), Italy (5), Germany (5), Belgium (4), Czech Republic (4), Poland (4) and Sweden (4).

465. The majority of requests sent were destined to Latvia (64), the UK (41), Estonia (29), Germany (26), Switzerland (19), Poland (19), Czech Republic (12), Cyprus (12), USA (10), Hong Kong (7), the UAE (7), Malta (7), the Russian Federation (6), France (6), the Netherlands (5) and Belize (5).

466. The authorities advised that most of the requests were answered within 20 days. There was only one refusal related to the FIU of Syria.

BoL:

467. The BoL makes full use of a large number of bilateral and multilateral agreements concluded with its foreign counterparts in order to exchange information (see Rec. 40, TC Annex).

468. The BoL also cooperates with its foreign counterparts in relation to AML/CFT on-site inspections upon invitation extended by a foreign supervisor. Supervisory colleges take place approximately 1-3 per year. After an invitation has been extended by a foreign supervisory authority, the BoL may undertake an AML/CFT on-site inspection to branches of foreign FIs in Lithuania. The BoL communicates to its foreign counterparts information on identified AML/CFT deficiencies, including recommended actions to rectify deficiencies.

469. Cooperation with international as well as EU institutions such as the European Banking Authority (EBA), the European Security and Market Authority (ESMA), the European Insurance and Occupations Pensions Authority (EIOPA) and the International Organisation of Securities Commission (IOSCO) is ongoing.

GCA:

470. The GCA cooperates with its EEA counterparts on the basis of a Cooperation Arrangement signed on the initiative of the Expert Group on Gambling (operating within the European Commission). The participation of the GCA in the Expert Group on Gambling and Gaming Regulators European Forum (GREF) provides a framework within which the GCA shares intelligence and expertise, including on AML/CFT. In addition, the GCA exchanges information and shares best practices through direct contacts, regional meetings and workshops. For instance, the GCA and its Baltic counterparts hold regular meetings to facilitate information exchange in relation to the implementation of the 4th EU Anti-Money Laundering Directive and other AML/CFT issues.

International exchange of basic and beneficial ownership information of legal persons and arrangements

471. The Lithuanian authorities (FIU, BoL, GCA, LEAs) confirmed that they regularly seek and provide basic and beneficial ownership (BO) information of legal persons. The feedback provided by the AML/CFT global network does not suggest particular concerns in this respect. However, the weaknesses identified under IO.5 could potentially affect the authorities' ability to exchange BO information.

472. The BoL exchanges basic and BO information on a regular basis with its EU and non-EU counterparts. Exchange of information usually relates to the criminal background of a legal person, its supervisory status and sanctions. Exchange of basic and BO information usually takes place during the licencing, registration, acquisition, or approval process. The BoL confirmed that in 2017 its licencing division contacted other foreign financial supervisory authority on 53 cases seeking for basic information on legal or natural persons (shareholders and/or managers), while over the same period it received 28 requests of the same nature. Also, the authorities informed that since the beginning of 2018, the BoL Licencing Division has addressed 47 BO requests to its foreign counterparts.

Table 34: BO-related incoming requests to the BoL

Year	Number of incoming requests	Execution time
2016	Approx.16	5-20 working days
2017	Approx.12	

Box 2.4 – Incoming BO request by a non-counterpart

The BoL advised that during 2018, it received a BO request (including information on managers/shareholders) from the US SEC in relation to a Lithuanian entity suspected of fraudulent activities. In its response, the BoL informed the US SEC that this entity had applied for a license in 2017, but a license had not been granted. The request was transferred to the FCIS which is currently conducting an investigation on the activities of the requested entity. The BoL informed the SEC that the FCIS is currently processing its request.

Conclusion

473. **Lithuania has achieved a substantial level of effectiveness with IO.2**.

TECHNICAL COMPLIANCE ANNEX

1. This annex provides detailed analysis of the level of compliance with the FATF 40 Recommendations in their numerological 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.

2. 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 2012. This report is available from https://rm.coe.int/report-on-fourth-assessment-visit-anti-money-laundering-and-combating-/16807168d6 .

Recommendation 1 - Assessing Risks and applying a Risk-Based Approach

3. Since these requirements were added to the FATF Recommendations in 2012, they were not assessed under the mutual evaluation of Lithuania in the previous round.

4. *Criterion 1.1* – Lithuania conducted its first national ML/FT risk assessment (NRA) in 2015. The methodology was developed by the FIU, with the expert assistance of a private consultancy firm. The authorities developed and distributed a questionnaire to FIs, DNFBPs, supervisors and LEAs. The purpose of the NRA was to "*identify, assess, and understand ML/FT risks*", as *"an essential part of the implementation and development of a national AML/CFT regime."* The NRA process was supervised by the high-level AML/CFT Coordination Group, created by Decree 42/2015 of the Prime Minister. The Group comprised senior officers from all AML/CFT public stakeholders. The final NRA report was approved in October 2015. It is not clear that Lithuania has identified and assessed all of the major ML/FT risks as noted under IO 1. For instance, there is no assessment of the types of products and services that may be misused for ML/FT purposes, the understanding of the degree to which cash may be used for ML/FT purposes due to ineffective measures in relation to the transportation of cash, the level of cross-border illicit flows was not considered to any degree, etc.

5. *Criterion 1.2* – The FCIS is the authority responsible for coordinating the ML/FT risk assessments (Art. 28 AML/CFT Law).

6. *Criterion 1.3* – Art. 28, AML/CFT Law states that *"the national risk assessment of money laundering and terrorist financing shall be carried out at least every four years."*

7. *Criterion 1.4* – The authorities advised that letters were sent to the supervisors and various relevant associations to make sure that their sectors are aware of the ML/FT risks identified in the NRA and the results of the EU supranational risk assessment. The NRA results have been published on the FIU website and are included in the regular training programmes implemented by the FIU and the BoL.

8. *Criterion 1.5* – Art. 26 AML/CFT Law states that the NRA findings/results shall be taken into account *"when planning the allocation of resources"* for AML/CFT *"and priorities for their use".* The NRA also states that its findings/results should assist the authorities in the prioritisation and efficient allocation of resources. Given the lack of granularity of the NRA and the incomplete understanding of risks, it is not clear how well Lithuania was able to allocate resources and implement measures to prevent or mitigate ML/FT.

9. *Criterion 1.6* – Lithuania does not exempt FIs or DNFBPs from applying some of the FATF Recommendations.

10. *Criterion 1.7* – The AML/CFT Law (Art. 29(3)) requires that internal controls of FIs and DNFBPs should be based on the supra-national risks assessment carried out at EU level and Lithuania's NRA. Additionally, enhanced CDD must be carried out where higher risk of ML/FT is identified based on the risks assessment and management procedures of the obliged entities.

11. *Criterion 1.8* – Art. 15 of the AML/CFT Law defines situations in which "simplified CDD" is permitted, referring, in general terms, to situations in which the lower risk of ML and/or FT is identified based on the risk assessment and management procedures established by obliged entities. Art. 15 also includes a list of customers and situations to which SCDD may be applied: i) companies whose securities are admitted to trading on a regulated market in one or more EU Member States; ii) public administration; iii) FIs covered by the AML/CFT Law or registered in another EU Member State; iv) life insurance contracts or supplementary voluntary pension accumulation agreements, where the annual premium does not exceed EUR 1,000; v) insurance policies for pension schemes where there is no surrender clause and where the insurance policies cannot be used as collateral; vi) pensions accumulated under the Law on Accumulation of Pensions; vii) e-money, where a limit of EUR 1,000 is imposed on the total amount transferred in a calendar year; viii) lotteries, where the monetary value intended for the purchase of lottery tickets and accumulation of unclaimed winnings is stored electronically, and the maximum monetary value stored does not exceed EUR 1,000; ix) when indicated by the European supervisory authorities and the EC; and x) deposits accepted from natural persons, with a limit of EUR 30,000. Art. 15(2), (3) and (4) sets specific conditions for the application of SCDD measures. It is unclear whether a lower risk has been identified with respect to the customers, products or situations included in Art. 15.

12. *Criterion 1.9* – The deficiencies under R.26 and 28 have an impact on Lithuania's compliance with this criterion.

13. *Criterion 1.10* – Art. 29 of the AML/CFT Law requires obliged entities to establish adequate risk assessment and management policies and control procedures, which need to take into account i) customer risk; ii) product or service risk and/or operational risk; and iii) country and/or geographical area risk. These policies and control procedures should be approved by senior management. As such, the AML/CFT does not specify that risk assessments must be documented, that all relevant risk factors should be considered or that assessments should be kept up-to-date. Moreover, although there is nothing which hinders the provision of information to competent authorities, there are no appropriate mechanisms in place.

14. *Criterion 1.11* – (a) Art. 29(1) of the AML/CFT law sets out the internal control procedures which obliged entities should have in place to assess and manage the risks. Art. 29(5) requires internal control procedures to be approved either by the senior manager or the management body of obliged entities. (b) Art. 29(6) of the AML/CFT law provides that obliged entities should monitor the implementation of internal control procedures and, where necessary, enhance them. In addition, Art. 26(4) states that obliged entities should have appropriate compliance and/or audit procedures to ensure the application of the AML/CFT Law requirements. (c) Art. 14(4) of the AML/CFT Law stipulates that enhanced CDD should be applied where a higher risk of ML/FT is identified through the risk assessment process carried out by the obliged entities. When assessing the risks of ML and/or FT, the following potentially higher risk factors should be assessed: customer; product, service, transaction or delivery channel; and geographical risk factors.

15. *Criterion 1.12* – Art. 15(1) of the AML/CFT law permits the application of simplified CDD (SCDD), where a lower risk of ML and/or FT is identified based on the risk assessment carried out by

obliged entities. The application of SCDD is limited to the cases listed in this article (see c.1.6). There are provisions which require the full application of CDD whenever there is a suspicion of ML/FT.

Weighting and Conclusion

16. Although Lithuania meets or mostly meets all criteria, two of the core criteria under R.1 (c.1.1 and 5) are rated as partly met. Therefore **R.1 is rated partially compliant (PC)**.

Recommendation 2 - National Cooperation and Coordination

17. In the 4th round MER Lithuania was rated PC with former R.31. The evaluation noted that no "effective mechanisms" were in place for AML/CFT domestic cooperation and coordination and questioned the outcome and effectiveness of the consultation mechanisms in place with the industry.

18. *Criterion 2.1* – While Lithuania does not have a national AML/CFT policy, following the completion of the NRA, an action plan was developed informed by the threats and vulnerabilities identified in the NRA. The authorities also referred to the different policy papers, strategies and activity plans, primarily produced by law enforcement, which define different priorities in combating serious crime, including ML/FT.

19. *Criterion 2.2* – The AML/CFT Coordination Group (see c.1.1) acts as a national coordination mechanism in the area of AML/CFT policy and risk mitigation. The Group meets twice a year to discuss the implementation of the NRA Action Plan. Extraordinary meetings could also be convened in case this is deemed necessary by any of its members.

20. *Criterion 2.3* – The AML/CFT Coordination Group enables policy makers and competent authorities to co-operate and where appropriate, co-ordinate domestically, with each other concerning the development and implement of policies and activities. Co-ordination of operational activities is done both at the level of the Group and bilaterally/multilaterally between the authorities depending on the area of co-operation.

21. *Criterion 2.4* – Although there is some co-operation in relation to proliferation matters, this is not the case for PF.

Weighting and Conclusion

22. In the absence of PF coordination mechanisms, **R.2 is rated PC.**

Recommendation 3 - Money laundering offence

23. In the 2012 MER Lithuania was rated PC with the previous R.1 and LC with the previous R.2. The gaps related to the physical elements of the ML offence and its scope.

24. *Criterion 3.1* – ML is criminalised under Art. 216(1) of the CC. The physical and mental elements required under the Vienna and Palermo Conventions are all present in the offence. Some minor deficiencies persist. The offence does not cover the conversion or transfer of property for the purpose of helping any person who is involved in the commission of the predicate offence to evade the legal consequences of his/her action. The acquisition, possession and use under Art. 216(1) are only criminalised insofar as they are committed with a concealment or legalisation purpose. This gap is largely mitigated by Art. 189 which criminalises the use and handling of stolen property. However, this article applies only to a person other than the person who committed the predicate offence.

25. *Criterion 3.2* – Lithuania applies an all-crimes approach. The ML offence refers to any property obtained by criminal means. The CC criminalises all the offences in each of the designated categories of offences (see table on p.41-42 of the 2012 MER) and also tax offences.

26. *Criterion 3.3* – (Not applicable).

27. *Criterion 3.4* – Pursuant to Art. 224[1] of the CC, the property referred to under the ML offence includes property of any form obtained directly or indirectly from a criminal act. The definition is wide enough to cover all different types of property referred to in the FATF Glossary. In addition, a definition based on the FATF Glossary is found in the AML/CFT Law.

28. *Criterion 3.5* – The ML offence does not require a conviction for the predicate offence. It simply refers to property obtained by criminal means. This has been confirmed in at least two Court of Appeal judgements (e.g. No. 1A-84/2013).

29. *Criterion 3.6* – As long as the property is obtained by criminal means, whether within or outside Lithuania, a person may be found guilty of the ML offence. This has also been confirmed by the courts (e.g. No. 1-29-290/2014).

30. *Criterion 3.7* – According to Art. 216(1) of the CC, a person shall commit ML if he conceals, transfers, uses, etc., his own property while being aware that it has been obtained by criminal means.

31. *Criterion 3.8* – Case law permits the mental element of the ML offence to be inferred from objective factual circumstances (e.g. No. 1A-84/2013).

32. *Criterion 3.9* – Sanctions are proportionate and dissuasive. The ML offence carries a maximum prison sentence of seven years or a maximum fine of EUR 300,000. ML is classified as a serious crime under the CC and the penalties for ML are similar to those applicable to other serious crimes.

33. *Criterion 3.10* – Legal persons are liable for ML (Art. 216(2) of the CC). The general concept of corporate criminal liability is covered under Art. 20 of the CC and appears to be sufficiently wide to comply with international standards (see para.91-92 of the 2006 MER).

34. *Criterion 3.11* – Ancillary offences are covered: participation (Art. 24(3) of the CC); conspiracy (Art. 21 of the CC); attempt (Art. 22 of the CC), aiding and abetting (Art. 24(5) and (6)); facilitating (Art. 24(6) of the CC); and counselling the commission (Art. 24(6) of the CC).

Weighting and Conclusion

35. Due to minor deficiencies in relation to the criminalisation of the ML offence, **R.3 is rated Largely Compliant (LC)**.

Recommendation 4 - Confiscation and provisional measures

36. Lithuania was rated LC with the previous R.3. As far as technical compliance is concerned, the rating was based on minor deficiencies related to confiscation and temporary measures.

37. *Criterion 4.1* – Confiscation is covered under Art. 72 of the CC, which has not changed since the 2012 MER, in which Art. 72 was considered compliant with these requirements (see par. 162-165).

38. *Criterion 4.2* – (a) During a pre-trial investigation, the prosecutor is required to take all necessary measures to identify and trace property that may be subject to confiscation (Art. 170[1] CPC). Prosecutors are required to conduct a parallel financial investigation to determine whether any

property has been obtained in a criminal or other unlawful way with a view to securing eventual confiscation (PG Rec. on Financial Investigations). (b) A prosecutor may order the provisional restraint of ownership rights for the purpose of securing a civil claim or probable confiscation of property (Art. 151 CPC). A detailed analysis of this article is set out in para.166-168 of the 2012 MER. No measures appear to have been taken to rectify the minor gap concerning the period of validity of a restraint order. It is not clear whether provisional measures can be made without prior notice in all cases. (c) This sub-criterion is met. See para.171 of the 2012 MER. (d) see c.4.2(a) and R.31.

39. *Criterion 4.3* – This criterion is met. See para.171 of the 2012 MER.

40. *Criterion 4.4* – There are mechanisms in place for the management and disposal of seized and confiscated property based on Gov. Res. No. 634 of 26 May 2004 and Art. 93(4) and (5) and Art. 94(1) CPC. The Resolution regulates the grounds, procedure and accounting of transfer of property and real evidence to the State Tax Inspectorate (Ch.I and II; Ch.III, Sec.I, II, VI, X), issues of realization of the property, sale of property by conducting a tendering procedure, under the agreements concluded on the basis of the tendering procedure, in electronic auctions, in electronic shops (Ch.IV, Sec.I, II, IV, V, VI, VII, VIII), storage of strategic goods, management of property recognized as waste (Ch.VI), return of property (Ch.VII) and distribution of received funds (Ch.VIII).

Weighting and Conclusion

41. **R.4 is rated LC**, due to minor deficiencies in relation to C.4.2.

Recommendation 5 - Terrorist financing offence

42. In the 2012 MER, Lithuania was rated PC with former SR.II, as some requirements were not covered (e.g. the collection of funds and support to individual terrorists, and also situations where funds have not actually been used for committing a terrorist acts or linked to a specific terrorist act).

43. *Criterion 5.1* – FT is criminalised as a stand-alone offence under Art. 250^4 of the CC and is broadly in line with the Standards. It refers to any person who directly or indirectly collects, accumulates or provides funds or other assets, or provides other material support, to another person, with the knowledge or intention that the assets, or part thereof, would (1) support or be used for the preparation or commission of a terrorist crime or a terrorist-related crime, or (2) support one or more terrorists, a terrorist group or a group that recruits or trains terrorists or otherwise participate in terrorist-related activities. A terrorist crime refers to acts set out under Art. 250 (acts of terrorism), Art. 251 (hijacking of aircraft, vessel, vehicle, fixed platform on the Continental Shelf) and Art. 252 (hostage taking), when committed for terrorist purposes. Crimes linked to terrorist activities are the crimes referred to in Art. 249^1, 250^1, 250^2, 250^3, 250^4, 250^5 and 250^6 CC, as well as in Art. 178, 180, 181 and 300 CC if they aim at obtaining funds, instruments or means to commit terrorist crimes or support activities of a terrorist group the purpose whereof is the commission of terrorist crimes. A terrorist purpose is defined as the intention to intimidate the public, unduly compel an international organisation, a government etc. Art. 250, 251 and 252 collectively broadly cover the offences within the scope of and as defined in the treaties annexed to the FT Convention. However, the financing of these acts is not entirely in line with Art. 2(1)(a) of the FT Convention as it is only criminalised insofar as these acts are committed with a terrorist purpose.

44. Art. 2(b) of the FT Convention is covered by reference to the financing of the acts set out under Art. 250(3) – causing serious health impairment to a person for terrorist purposes – and Art. 250(4) –

killing one or more persons for terrorist purposes. This formulation does not exclude persons not taking an active part in the hostilities in a situation of armed conflict.

45. *Criterion 5.2* – As indicated under c.5.1, the FT offence applies to the collection and provision of funds or other assets (1) to support or be used for the preparation or commission of a terrorist crime or a terrorist-related crime, or (2) support one or more terrorists, a terrorist group or a group that recruits or trains terrorists or otherwise participate in terrorist-related activities. While there is no definition of a terrorist group, the CC criminalises the establishment, participation in the activities, and the organisation of a group having the aim of committing terrorist crimes (Art. 249^1). Additionally, the FT offence itself criminalises the financing of a group that recruits or trains terrorists or otherwise participates in terrorist-related activities. There is nothing in the wording of Art. 250^4 which suggests that the financing of a terrorist or a terrorist group must be linked to a specific terrorist act.

46. *Criterion 5.2bis* – Art. 250^4 of the CC criminalises the financing of terrorist-related crimes, which, according to the interpretation provided in Art. 252^1, include travelling for terrorist purposes, criminalised as a separate offence under Art. 250^6 and training of terrorists, criminalised as a separate offence under Art. 250^5.

47. *Criterion 5.3* – Art. 250^4 of the CC does not distinguish between funds or other assets from legitimate or illegitimate sources.

48. *Criterion 5.4* – The FT offence does not require that funds or other assets are actually used to carry out or attempt a terrorist act or be linked to a specific terrorist act.

49. *Criterion 5.5* – The CC does not regulate the conditions for proving the intent, which is left in the hands of the courts. While there is no court practice with respect to FT offences, case law exists which indicates that intent and knowledge may be inferred from objective factual circumstances (see c. 3.8).

50. *Criterion 5.6* – FT is considered to be a grave crime (Art. 11(5) CC) and is punished solely by a custodial sentence for a term of up to ten years.

51. *Criterion 5.7* – Pursuant to Art. 250^4(2) of the CC, a legal entity shall also be held liable for the acts provided for in that article. Grounds and conditions for a legal person's criminal liability are set out in Art. 20 CC. See c.3.10.

52. *Criterion 5.8* –See c.3.11.

53. *Criterion 5.9* – Lithuania applies an all-crime regime, which also includes FT.

54. *Criterion 5.10* – Art. 250^4 of the CC does not link the commission of FT with a particular terrorist organisation or its location. Furthermore, according to Art. 7(10) of the CC, persons shall be liable under the CC for terrorist crimes and terrorist-related crimes, including FT, regardless of their citizenship and place of residence, also of the place of commission of a crime and whether the act committed is subject to punishment under laws of the place of commission of the crime where they commit acts of terrorism and crimes related to terrorist activity.

Weighting and Conclusion

55. Due to minor deficiencies in relation to the criminalisation of FT, **R.5 is rated LC**.

Recommendation 6 - Targeted financial sanctions related to terrorism and terrorist financing

56. In the 2012 MER, Lithuania was rated PC with previous SR.III. Assessors identified the following deficiencies: unclear mechanisms to challenge domestic and EU decisions; insufficient public information and guidance on the specificities of the international sanctions mechanisms (as opposed to the STR system); Effectiveness of supervision, coordination and monitoring of implementation was not demonstrated; the authorities were themselves not familiar with the applicable rules.

57. As an EU member state, Lithuania is bound by the EU legal instruments which implement UNSCRS: Reg. 881/2002 (UNSCR 1267/1989), Reg. 753/2011 (UNSCR 1988) and Reg. 2580/2001 and Common Position 2001/931/CFSP (UNSCR 1373). The EU framework is supplemented at the national level by the FIU Instructions on Sanctions, which apply only upon the coming into force of designations made at EU level.

58. *Criterion 6.1* –

(a) The authorities state that the MFA has responsibility for proposing person or entities to the 1267/1989 and 1988 Committees. However, there appears to be no internal regulations within the Ministry which specifically set out this responsibility.

(b) The SSD actively monitors the territory of Lithuania to identify persons with links to terrorism or FT. However, it appeared that the SSD was not aware of the obligation to identify targets based on the designation criteria set out in the relevant UNSCRs.

(c) to (e) Lithuania has no mechanisms and procedures in place to comply with these requirements.

59. *Criterion 6.2* –

(a) At the EU level, the EU Council is responsible for deciding on designations. EU listing decisions would be taken on the basis of precise information from a competent authority, i.e. a judicial authority or equivalent of an EU Member State or third state. The MFA would (*purportedly*) be the competent authority that would refer the proposal to designate to the EU Council.

(b) See 6.1(b).

(c) The COMET Working Party at the EU Council examines the requests received at the European level to determine whether they are supported by reasonable grounds and meet the criteria set forth in UNSCR 1373. The criteria set forth in CP 2001/931/CFSP are compliant with those stipulated in UNSCR 1373. All Council working parties consist of representatives of the governments of the Member States. There is no requirement that a prompt determination is made.

(d) The COMET WP applies an evidentiary standard of proof of 'reasonable basis' and the decision is not conditional on the existence of criminal proceedings (Art. 1(2) and (4) CP 2001/931/CFSP). It is not clear what happens with respect to requests received by Lithuania.

(e) There is no procedure detailing steps to be taken in cases where Lithuania makes a request to another country for listing.

60. *Criterion 6.3* – The SSD and the Police may collect or solicit information pursuant to the Law on Criminal Intelligence and operate ex parte (Art. 4 and 6).

61. *Criterion 6.4* – The implementation of TFS set out under UNSCRs 1267/1989 and 1988 into the EU framework does not take place 'without delay', since there is a delay between the designation decision taken by the UNSC and its transposition into the EU framework. The delay is caused by the application of a due diligence process in light of case law of the European Court of Justice leading to the adoption of a legally binding act to be published in the EU Official Journal. The implementation of TFS set out under UNSCR 1373 under the EU framework takes place 'without delay'. As for UNSCR 1373 the implementation of designations based on requests from another country, it is not clear what mechanism would apply.

62. *Criterion 6.5* –

(a) Natural and legal persons in Lithuania are required to freeze funds and other assets under UNSCRS 1267/1989 and 1988 only when such obligations are transposed into the EU framework. As noted under c.6.4, designations are not transposed into the EU framework without delay and, as such, it is doubtful whether, in practice, the freezing action takes place without prior notice. Both issues create a significant gap within the framework. Under UNSCR 1373, the obligation to freeze funds and other assets applies immediately to all EU Member States and without prior notice. EU internals are covered under clauses 5.1 and 5.2 of the FIU Instructions.

(b) Pursuant to UNSCR 1267/1989 and 1988, the freezing obligation extends to all the funds or other assets defined in R.6, namely funds owned by designated persons (natural or legal) as well as funds controlled by them or by persons acting on their behalf or on their orders. These aspects are covered by the notion of "control" in Art. (2) of Reg. 881/2002 Art. 3 of Reg. 753/2011. The definition of "funds or other assets" was amended to include economic resources pursuant to Art. 1 of Reg. 2016/1686 (applying additional restrictive measures against ISIL (Da'esh) and Al-Qaeda). With regard to UNSCR 1373, the freezing obligation under Art. 2(1)(b) of Reg. 2580/2001, and under the RD of 28 December 2006, is not extensive enough as it does not cover the issue of "control". Technically, this issue does not arise in Lithuania, since Clauses 5.1 and 5.2 require persons to apply the sanctions in the manner as set out under the UNSCRs.

(c) At the EU level and in compliance with the UNSCRs, the regulations prohibit EU nationals and all other persons or entities present in the EU from making funds or other economic resources available to designated persons or entities.

(d) Designations made pursuant to the EU regulations are published in the Official Journal of the EU (publicly available on the EURLEX website) and on the website of the European External Action Service (users may subscribe to an automatic alert notification). The European Commission updates the Financial Sanctions Database after the issuing of UN designations and after publication of a listing in the Official Journal. The financial sector and DNFBPs can subscribe to the RSS-file with the latest updates. Credit institutions can also download the consolidated list through ftp access. There are no other communication mechanisms in place, except for periodic notices circulated by the FIU, which do not fulfil the requirement that updates are communicated immediately. No guidance has been issued.

(e) FIs and DNFBPs are required to notify the FIU, Customs and the CBL whenever freezing is applied (Clause 5.7, FIU Instructions).

(f) The EU framework provides for the protection of bona fide third parties: Reg. 881/2002 (Art. 6), Reg. 753/2001 (Art. 7), Reg. 2580/2001 (Art. 4).

63. *Criterion 6.6* –

(a) There are publicly-known procedures to submit de-listing requests to the Office of the Ombudsperson of the UN Security Council (Al-Qaida and ISIL designations) and the Focal Point for De-Listing (Taliban designations)(Clause 10, FIU Instructions). Designated persons are instructed to refer their petitions directly to the Ombudsman and the Focal Point. Lithuania has not, however, decided that, as a rule, its citizens or residents should address their de-listing requests directly to the Focal Point through a declaration addressed to the Chairman of the Committee (footnote 1 of UNSCR 1703).

(b) Under UNSCR 1373, the EU Council regularly revises the list (at least every six months – Art. 6 of the CFSP) in accordance with the assessment of the COMET WP. The FIU instructions further explain the steps to be taken by an entity for de-listing and un-freezing (Clause 12, FIU Instructions).

(c) At the EU level, a listed individual or entity can write to the Council to have the designation reviewed or can challenge the relevant Council Regulation, a Commission Implementing Regulation, or a Council Implementing Regulation in Court, as per Treaty on the Functioning of the European Union (TFEU) (Art. 263 (4)). Art. 275 also allows legal challenges of a relevant CFSP Decision.

(d) The FIU Instructions state that persons listed pursuant to UNSCR 1988 may apply to the Focal Point for De-listing of the UNSC and provide a link to the relevant website (Clause 10.2).

(e) The FIU Instructions state that persons listed pursuant to the Al-Qaida/ISIL (Da'esh) Sanctions Lists shall be entitled to file requests to the Office of the Ombudsperson of the UNSC and provide a link to the relevant website.

(f) – *(g)* There are no procedures fulfilling these requirements.

64. *Criterion 6.7* – At both the EU and domestic level, there are mechanisms for authorising access to frozen funds or other assets which have been determined to be necessary for basic expenses, the payment of certain types of expenses, or for extraordinary expenses: Reg. 881/2002 (Art. 2a), Reg.753/2011, Reg.2580/2001 (Art. 5-6), FIU instructions (Clauses 9, 12.3, 13 and 14).

Weighting and Conclusion

65. There appears to be no internal regulations within the MFA which specifically set out this responsibility. The SSD actively monitors the territory of Lithuania to identify persons with links to terrorism or FT. However, it appeared that the SSD was not aware of the obligation to identify targets based on the designation criteria set out in the relevant UNSCRs. Lithuania has no mechanisms and procedures in place to comply with these requirements. There is no requirement that a prompt determination is made. It is not clear what happens with respect to requests received by Lithuania. There is no procedure detailing steps to be taken in cases where Lithuania makes a request to another country for listing. The implementation of TFS set out under UNSCRs 1267/1989 and 1988 into the EU framework does not take place 'without delay', since there is a delay between the designation decision taken by the UNSC and its transposition into the EU framework. It is doubtful whether, in practice, the freezing action takes place without prior notice. There are no other communication mechanisms in place, except for periodic notices circulated by the FIU, which do not fulfil the requirement that updates are communicated immediately. No guidance has been issued. Lithuania has not, however, decided that, as a rule, its citizens or residents should address their de-listing requests directly to the Focal Point through a declaration addressed to the Chairman of the Committee. There are no procedures fulfilling these requirements. **R.6 is rated PC**.

Recommendation 7 – Targeted financial sanctions related to proliferation

66. Lithuania's previous ME was conducted prior to FATF's 2012 adoption of R.7

67. As an EU Member State, Lithuania implements UNSCRs through the EU legal framework. The implementation of targeted financial sanctions is additionally regulated by the Law on Sanctions and the FIU Instructions on Sanctions. UNSCR 1718 on the Democratic People's Republic of Korea (DPRK) is transposed into the EU legal framework through Council Reg. 329/2007, Council Decision (CD) 2013/183/CFSP, and CD 2010/413. UNSCR 1737 on Iran is transposed into the EU legal framework through Council Reg. 267/2012.

68. *Criterion 7.1* – Although EU Regulations are implemented immediately in all EU Member States upon the publication of decisions in the EU Official Journal, there are delays in the transposition into European law of UN decisions on DPRK, which is mitigated by the significant number of other designations by the EU. With regard to Iran, the technical problems in the EU for the transposition of UN sanctions and any delays which might have occurred after such transposition have not in practice led to any delays in the implementation of TFS related to PF.

69. *Criterion 7.2* –

(a) The same shortcomings noted under C.6.5(a) apply.

(b) The freezing obligation applies to all types of funds.

(c) Art. 6.4 of Regulation 329/2007 and Art. 23.3 of Regulation 267/2012 prohibit making available, directly or indirectly, funds or economic resources to designated persons or entities or for their benefit, unless otherwise authorised or notified in compliance with the relevant UNSCRs.

(d) The same shortcomings noted under c.6.5(d) apply.

(e) See c.6.5(e).

(f) The rights of bona fide third parties are protected by the relevant EU Regulations (Art. 11 of Reg. 329/2007 and Art. 42 of Reg. 267/2012).

70. *Criterion 7.3* – Sanctions for non-compliance with UNSCRs 1737 and 1718 are provided for in EU (Restrictive Measures concerning Iran) Regulations 2016 (Statutory Instrument No. 478 of 2016) and EU (Restrictive Measures concerning the Democratic People's Republic of Korea) (No. 2) Regulations 2016 (Statutory Instrument No. 540 of 2016) respectively. In both cases, persons who fail to comply are subject to a class A fine (up to EUR 5,000) or imprisonment for a term not exceeding 12 months or both; or on conviction on indictment, to a fine not exceeding EUR 500,000 or to imprisonment for a term not exceeding 3 years or both (Regulations 4-6 and Regulation 4, respectively). Monitoring is performed during FIU and BoL on-site inspections.

71. *Criterion 7.4* –

(a) The EU Council communicates its designation decisions, and the grounds for inclusion, to the designated persons or entities which have the right to comment on them. If this is the case or if new substantial proof is presented, the Council must reconsider its decision. Individual de-listing requests must be processed upon receipt, in compliance with the applicable legal instrument and EU Best Practices for the effective implementation of restrictive measures. Designated persons or entities are notified of the Council decision. Delisting requests may be directly filed with the EU Council or the competent UN authority (Focal Point established pursuant to UNSCR 1730). When the UN decides to

de-list a person, the EC modifies the lists in the annexes of the EU Regulations without the person in question having to request it (Art. 13.1(d) and (e) of Reg. 329/2007, and Art. 46 of Reg. 267/2012). Persons and entities affected by restrictive measures may file a delisting petition with the competent national authorities that will channel such request to the respective institutions. Designated persons or entities individually affected may also institute proceedings before the European Court of Justice to challenge the relevant (EU) Sanctions Regulations.

(b) Publicly known procedures are available for obtaining assistance in verifying whether persons or entities are inadvertently affected by a freezing mechanism having the same or similar name as designated persons or entities (i.e. a false positive).

(c) At the EU level, there are specific provisions for authorizing access to funds or other assets, where the competent authorities of Member States have determined that the exemption conditions set out in UNSCRs 1718 and 1737 are met, and in accordance with the procedures set out in those resolutions. EU implementing regulations provide mechanisms for authorising access to frozen funds or other assets which have been determined to be necessary for basic expenses, the payment of certain types of expenses or for extraordinary expenses. Any of the three competent authorities may authorise, under such conditions as deemed appropriate, the release of certain frozen funds or economic resources, if the competent authority determines that the EU Regulation conditions have been met. Applications for such authorizations should be made in writing.

(d) The procedures set out in C.6.5(d) are equally applicable to any changes to EU listings, which will be given effect to by a Council Regulation or a Council/Commission Implementing Regulation, notice of which will appear in the Official Journal and will be communicated by DFAT to the members of the CDISC. Notice will, in turn, appear on the website of the Competent Authorities.

72. *Criterion 7.5* –

(a) Art. 9 of Reg. 329/2007 and Art. 29 of Reg. 267/2012 permit the payment to the frozen accounts of interests or other sums due on those accounts or payments due under contracts, agreements or obligations that arose prior to freezing, provided that these amounts are also subject to freezing.

(b) Art. 24-25 of Reg. 267/2012 authorise the payment of sums due under a contract entered into prior to the designation of such person or entity, provided that this payment does not contribute to an activity prohibited by the Regulation, and after notice is given to the UN Sanctions Committee.

Weighting and Conclusion

73. In general, as with R.6, Lithuania's compliance with R.7 is limited by uncertainties and gaps in its legal basis. There are delays in the transposition into European law of UN decisions on DPRK, which is mitigated by the significant number of other designations by the EU. Shortcomings noted under C.6.5 impact C.7.2. **R.7 is rated PC**.

Recommendation 8 – Non-profit organisations

74. In the 2012 MER, Lithuania was rated PC with former SR.VIII. The main deficiencies were: no review of the NPO sector in respect of its misuse for FT; lack of outreach to NPOs; gaps in the legal framework in respect of financial transparency and record keeping and updating; no effective implementation of NPOs' compliance with their legal obligations in all cases and partial oversight relying to a large extent on the taxation supervision.

75. *Criterion 8.1* –

a) A NPO FT risk assessment was performed in 2017, including the identification of the subset of organisations that fall within the FATF definition and those NPOs that are more likely to be at risk of FT abuse. In particular, the 2017 Strategic Analysis was based on STRs in relation to NPOs, which had cashed out more than EUR 80,000.

b) Lithuania has taken steps to identify the nature of FT threats to NPOs and how terrorist actors abuse those NPOs. As a result of the Strategic Analysis, the SSD received and analysed information in relation to the financial activity of 18 NPOs. The SSD has also confirmed that it monitors approximately 30 religious NPOs vulnerable to FT.

c) Lithuania has not reviewed the adequacy of its measures that relate to the subset of the NPO sector that may be abused for FT support. However, as per the NRA Action Plan, the FCIS has updated the list of criteria for the NPOs' assessment when there are indications of potential ML/FT in their activities. Mitigating measures on risk related to NPOs are also included in the STI Action Plan.

d) The NRA assessed the ML/FT risk of domestic NPOs to be of medium priority. Since 2015 Lithuania reassessed its NPO sector during the 2017 Strategic Analysis, which is the first of a series of annual reviews to follow.

76. *Criterion 8.2* –

a) Although there is no specific policy document on the promotion of transparency, integrity and public confidence in the administration and management of NPOs, legal requirements can be found in the Law on Charity and Sponsorship Funds, the Law on Public Establishments and the Law on Associations. In particular, the Law on Charity and Sponsorship Funds requires NPOs to submit annual financial statements or, where an audit has been conducted, an audited set of annual financial statements together with the auditor's opinion (and a report on activities and an annual report of a public establishment) to the manager of the RLE. The documents submitted to the manager of the RLE shall be published free of charge in its website no later than within 30 days (Art. 12(4)). In addition, providers of sponsorship are obliged to submit annual reports to the STI on the sponsorship provided, and monthly reports when the amount of support provided to one beneficiary from the beginning of the calendar year exceeds EUR 15,000 (Art. 11(1)). Legal persons who receive sponsorship are also obliged to submit monthly and annual reports to the STI on the sponsorship they have received and its use, sponsorship and/or charity provided by themselves, as well as their activities relating to the achievement of purposes beneficial to the public (Art. 3(3)).

b) No specific outreach to NPOs and donors in relation to FT has taken place.

c) The NPOs sector has not been involved in any activity to develop and refine best practices to address FT risk and vulnerabilities.

d) There is no legal requirement or public policy paper encouraging NPOs to conduct their transactions via regulated financial channels.

77. *Criterion 8.3* – The supervision of NPOs is performed by the STI and the FCIS (Order No V-85/V-267 of the Director of the FCIS and the Head of the STI of 10 September 2010). The tax inspection procedures on NPOs mirror the STI's competences in respect to tax law. When FT indicators or other criminal offences are identified during tax inspections, The STI directly informs the FCIS and the competent LEAs (Art. 127 (2) of the Law on Tax Administration). NPOs have to be registered with the RLE in the same way as private companies (Art. 2.62, 2.66, 2.71 of the Civil Code). As of March 2010

all data on NPOs available to the RLE are available to the public (Resolution of the Government No. 1407 (12-11-2010)). The RLE contains complete information (and historical data) about the legal form and the status of legal entities, the fields of activity, the size and the structure of the authorised capital, the members of sole and collective management bodies, the licenses acquired, etc. The RLE virtually implements the policy of transparency of Lithuanian businesses, institutions and NPOs since all the data and information mentioned above is public. Excerpt from the registry of any legal entity as well as annual financial statements, lists of shareholders or copies of any other document (such as memorandum of foundation or board minutes) stored in the archive of the RLE are accessible by anybody for the fee set by the Government. The Law on Charity and Sponsorship Funds (Art. 11(2)) provides for all targeted risk-risk-based measures under R.8.

78. In 2017, the FCIS amended the list of criteria for the NPOs' when reviewing their monetary operations or transactions (Order No V-76). In the aftermath of the 2017 Strategic Analysis, information related to the financial activity of 38 and 18 NPOs, were communicated to the regional board of the FCIS and the SSD respectively.

79. *Criterion 8.4* –

a) Information on NPOs is publicly available in the RLE. The STI pays particular attention to the monitoring of NPOs in relation to taxation. General reporting requirements and risk-based measures are applied to them (see C.8.3). According to the STI Action Plans (2013-2014; 2014-2015; 2016-2017; 2018-2019), particular mitigating measures are taken in relation to NPO abuse. The Action Plan is periodically revised in order to list major threats to tax collection, identify shadow economy activities (risk types), provide for the targets to be achieved and priority activities for their implementation and eventually ensure tax collection. The FCIS has adopted and updated criteria for the NPOs' assessment when there are indications of possible ML/FT in their activities.

b) Under the Code of Administrative Offences, breaches of requirements on registration, the provision of information to the RLE and financial reporting are liable to fines. Art. 13 (5) of the Charity and Sponsorship law prescribes the procedures for annulling the status of a sponsorship recipient upon the recommendation of the control institution, e.g. after having established that the recipient has committed a violation of the AML/CFT law. Under Art. 205 and 223 of the Code of Administrative Offences a warning is imposed for violations of accounting laws or submission of false financial statements. Art. 12(3) of the Charity and Sponsorship law grants the power to the STI to cancel tax reliefs and impose statutory sanctions when identifying violations in respect of the provision, receipt and use of charity and sponsorship. In addition, the STI can impose administrative tax fines from 10 to 50% of the non-calculated taxes, including late payment interest (Art. 96 and 139 of the Law on Tax administration).These sanctions do not preclude the imposition of criminal sanctions under the CC. If a person is fined according to the CC, the tax administrator, for the same violation, can only calculate non-calculated taxes and late payment interest (in such cases the tax administrator does not impose penalties).

80. *Criterion 8.5* –

a) General reporting obligations for NPOs are in place. The majority of data regarding NPOs can be found in the RLE, which is accessible to the general public free of charge through an electronic portal. The legal framework provides for co-operation, co-ordination and information sharing among all relevant authorities. Art. 30(1) of the Law on Tax Administration establishes that the tax administrator cooperates with other state or municipal institutions, exchanges information and conducts joint inspections with other institutions. Art. 127(2) stipulates that any acts that may be

considered criminal or any other offence, in the course of an audit, should be referred to the relevant law enforcement or controlling authority for further investigation.

Rules approved by Order No. 7-V/V-28 of the Director of the FCIS and the Head of the STI (as amended in 2010 by Order No V-85/V-267), provides for STI-FCIS cooperation, including on AML/CFT issues. As per the Order, the STI informs the FCIS about possible criminal activity and activity which has indicators of criminal offenses for the financial system, including cases of potential ML/FT. The FCIS also provides information to the STI on potential violations of tax laws, including potential ML cases. The FCIS list of criteria for the NPOs' assessment, when there are indications of potential ML/FT in their monetary operations or transactions, governs the AML/CFT STI-FCIS cooperation. According to the STI and the FCIS Agreement for data submission, information exchange refers to tax payers' records, and monetary operations and transactions. This data is used for identification of risky taxpayers and individual assessment and control of taxpayers, as well as for performing thematic analysis. The taxpayers register data shall automatically be shared in accordance with data provision contracts. ML cases are analysed and decisions made by the Risk Analysis Centre. Intelligence on FT is collected and analysed by the SSD (Art. 6 of the AML/CFT Law).

b) In the area of CFT Lithuania established a clear framework for information exchange among relevant authorities and monitoring of the NPO sector (Art. 6 and 16 AML/CFT Law and Art. 18 of the Law on Intelligence). STI officials, who conduct the actions of control, are introduced the FCIS list of criteria for the NPOs' assessment. However, beyond the FCIS List, trainings or education activities to update and enrich the expertise of all those involved in FT-related NPO investigations are very rare.

c) Full information on the administration and management of particular NPOs is accessible in a timely manner, given that relevant information is stored publicly and is easily accessible. In addition, the Law on Tax Administration[80] (Art. 33) empowers tax administrators to obtain data required, copies of documents, computer file data concerning the assets, income, expenses and activities of legal persons and use information from the registers and databases administered and managed by itself or other legal persons.

d) Lithuania has in place a legal framework to ensure that information is shared between competent authorities. Art. 6(2) AML/CFT Law provides for information exchange in relation to CFT between the SSD and the FCIS. Pursuant to Art. 8 state institutions not conducting criminal prosecution shall report any observed acts of potential ML/FT to the FCIS. Art. 18 of the Law on Intelligence requires the SSD to provide intelligence information to LEAs for the purpose of initiation of criminal intelligence investigations or criminal proceedings.

81. *Criterion 8.6* – Exchange of information with foreign counterparts of the FCIS and the BoL is provided based on Art. 5 (6) and Art. 8 (2) of the AML/CFT respectively. The STI can exchange information with foreign state institutions (Art. 28 to 30 of the Law on Tax Administration). In addition, Art. 18 of the Law on Intelligence obliges the SSD to provide intelligence to international organisations and institutions, and competent authorities of foreign states, where the possibility of providing such information is established in international treaties or agreements.

Weighting and Conclusion

[80] Authorities please provide the relevant Article in the Law.

82. Lithuania reviewed its NPO sector. However, it has not reviewed the adequacy of its measures that relate to the subset of the NPO sector that may be abused for FT support. There is no specific outreach to NPOs and donors in relation to FT. The NPOs sector has not been involved in any activity to develop and refine best practices to address FT risk and vulnerabilities. There is no legal requirement or public policy paper encouraging NPOs to conduct their transactions via regulated financial channels. Beyond the FCIS List, trainings or education activities to update and enrich the expertise of all those involved in FT-related NPO investigations are very rare. **R.8 is rated LC**.

Recommendation 9 – Financial institution secrecy laws

83. Lithuania was rated LC with former R.4 in the 4th round MER. The underlying factors for the rating were: no harmonisation of the provisions under the respective laws lifting confidentiality; and no explicit requirement enabling the disclosure of AML/CFT-related information between the supervisory authorities. Since the previous evaluation, the AML/CFT Law has been amended.

84. *Criterion 9.1* – There are no secrecy provisions which inhibit the implementation of the FATF Recommendations. Sectorial laws, such as the Law on Banking and other similar laws regulating FIs, contain provisions which state that financial secrecy provisions do not prejudice access to information required by competent authorities to perform their functions (see e.g. Art. 55(3) of the Law on Banks). There is a similar provision in Art. 23(8) of the AML/CFT Law applying to the FCIS. However, there is nothing which covers the issue of R.13, 16 and 17.

Weighting and Conclusion

85. C.9.1 is met. **R.9 is rated Compliant (C)**.

Recommendation 10 – Customer due diligence

86. In the 2012 MER, Lithuania was rated PC with R.5, due to the lack of explicit requirements to understand the ownership and control structure of customers that are legal persons and review existing records for higher risk customers or business relationships; deficiencies in internal control; and the absence of clear legal provisions on the timing of verification. Weaknesses in the effective implementation of BO identification and verification obligations were also noted.

87. *Criterion 10.1* – An explicit prohibition to issue anonymous passbooks or open anonymous accounts or accounts in manifestly fictitious names is set out in the AML/CFT Law. The AML/CFT guidelines for FIs requires FIs to pay special attention to ML/FT threats related to the cases where it is intended to conceal the customer's or the BO's identity (in favour of anonymity).

88. *Criterion 10.2* – According to Art. 9 of the AML/CFT Law, FIs must take measures and identify the customer and BO as well as verify their identity:

1) prior to establishing a business relationship;

2) prior to carrying out one-off or several interlinked monetary operations or concluding transactions amounting to EUR 15,000 or more, or an equivalent amount in a foreign currency, irrespective of whether the transaction is carried out in a single operation or in several interlinked operations, except where the identity of the customer and the BO has already been established; however, the definition of monetary operations exempts payments to state and

municipal institutions, other budgetary institutions, the BoL, state or municipal funds, foreign diplomatic missions or consular posts or settlement with these entities.

3) when executing and accepting money transfers in compliance with Regulation (EU) No 847/2015 of the European Parliament and of the Council of 20 May 2015 on information accompanying transfers of funds (EU Reg. 847/2015);

4) when there are doubts about the veracity or authenticity of previously obtained identification data of the customer and of the beneficial owner;

5) in any other case, when there are suspicions that ML and/or FT is, was or will be carried out.

89. *Criterion 10.3* – According to Art. 9(15) of the AML/CFT Law, FIs are required to verify the identity of the customer on the basis of the documents, data or information obtained from a reliable and independent source. However, the definition of customer excludes state and municipal institutions, other budgetary institutions, the BoL, state or municipal funds, foreign diplomatic missions or consular posts.

90. *Criterion 10.4* – According to Art. 10(4) of the AML/CFT Law, when the customer is a legal or natural person represented by a natural person, the identity of the representative shall be established in the same manner as the identity of the customer that is a natural person (in the physical presence of the customer). In addition, the FI must ask for the power of attorney and verify its validity (*i.e.*, the right of the person who has issued it to issue such a power of attorney), its period of validity and the actions to be taken as specified in the power of attorney. Verification is covered under Art. 10(4) and (3) and 9(15) of the AML/CFT Law. There are no provisions related to the identification of representatives of legal arrangements.

91. *Criterion 10.5* – Pursuant to Art. 9(1) and (15), FIs must identify and verify the identity of BOs on the basis of documents, data and information obtained from a reliable and independent source. Art. 12 goes into further detail on how to identify and verify the identity of the BO. In a limited number of situations set out under Art. 15(1), where a lower risk of ML/FT is identified based on FIs' risk assessment and management procedures, simplified CDD may be applied. In these cases, FIs should identify, but need not verify, the identity of the BO. However, where in the course of on-going monitoring it is determined that the risk is no longer low, FIs should then proceed with the verification of the identity of the BO (Art. 15(7)).

92. *Criterion 10.6* – FIs must obtain information from the customer on the purpose and intended nature of the customer's business relationships (in all cases where CDD is applied). The AML/CFT Law does not contain an obligation to *understand* the purpose and intended nature of the relationship, however this requirement is found in the Guidelines for Financial Market Participants (Para. 29).

93. *Criterion 10.7* – FIs must carry out on-going monitoring of the customer's business relationships, including scrutiny of transactions, to ensure that the transactions are consistent with the FIs' knowledge of the customer, its business and risk profile as well as the source of funds. The documents, data or information submitted by the customer and the BO during CDD must be regularly reviewed and kept up-to-date.

94. *Criterion 10.8* – FIs must gather from the customers that are legal persons documents and additional data to satisfy themselves that they understand the management structure and the nature

of activities of the customer. Such obligations do not cover customers that are legal arrangements. There are no obligations to understand the ownership or control structure.

95. *Criterion 10.9* – As per Art. 10(2) and (3) of the AML/CFT Law, when identifying legal persons, FIs shall require the customer to provide documents or copies with a notarial certificate including name; legal form, registered office and address of operations; registration number; and an extract of registration and its date of issuance. The customer must also provide the name and other identification elements of the director of the legal person (*this does not include the powers that regulate and bind the legal person*). For the verification requirements, the authorities indicate that the analysis under c.10.3 applies. There are no specific requirements related to legal arrangements.

96. *Criterion 10.10* – The BO must be identified as described under c.10.5. The BO is defined by the AML/CFT Law as any natural person who owns the customer (a legal person or a foreign undertaking) or controls the customer and/or the natural person on whose behalf a transaction or activity is being conducted. The BO includes the natural person who owns or manages the legal person through direct or indirect ownership of a sufficient percentage of the shares or voting rights, or has control via other means. A shareholding of 25% plus one share or an ownership interest of more than 25% in the customer held by a natural person shall be an indication of direct ownership. A shareholding of 25% plus one share or an ownership interest of more than 25% in the customer held by an undertaking, which is under the control of a natural person(s), or by multiple undertakings, which are under the control of the same natural person(s), shall be an indication of indirect ownership. If no such person is identified, or if there is any doubt that the person identified is the BO, the natural person who holds the position of senior managing official shall be identified.

97. *Criterion 10.11* – In the case of a trust, identification and verification shall include: the settlor; the trustee; the protector (if any); the natural person benefiting from the legal person or entity; or - where such a person has yet to be determined - the group of persons in whose main interest the trust is set up or operate; any other natural person exercising ultimate control over the trust by means of direct or indirect ownership or by other means. In the case of an entity similar to a trust – the natural person holding an equivalent position as above (Art. 9(8) of the AML/CFT Law).

98. *Criterion 10.12* – Insurance undertakings and brokerage firms engaged in life insurance activities shall additionally establish and verify the identity of the beneficiary. In the case of beneficiaries that are designated by characteristics or by class or by other means, sufficient information shall be gathered to satisfy FIs that they will be able to establish the identity of the beneficiary at the time of pay-out. In case of beneficiaries that are identified as specific persons, the following shall be required: for natural persons - name, surname and personal number (or the date of birth, or the number of residence permit in Lithuania); for legal persons: name, registration number, legal form and registered office/address. Verification should occur at the time of pay-out or at the time the beneficiary intends to exercise the rights to payments vested under the policy.

99. *Criterion 10.13* – As part of enhanced CDD (Art. 14 of the AML/CFT Law), FIs involved in life insurance business shall, at the time of pay-out, determine whether the beneficiary can be considered as presenting a higher risk of ML and/or FT. Where the beneficiary is a legal person or an entity not having legal personality, the BO must, pursuant to Art. 12, be established before pay-out. Art. 9.6 does not specify whether it is a legal person or arrangement so it applies to both.

100. *Criterion 10.14* – As a general rule, FIs must identify the customer and BO and verify their identity prior to establishing a business relationship; or prior to carrying out one-off or several interlinked monetary operations or concluding transactions amounting to EUR 15,000 or more. FIs

may establish a business relationship with customers without verifying their identity if: monetary operations will not be carried out in such an account until customer identification and verification are complete; and CDD is finalised not later than within one month from the date of opening of the account. In such cases FIs must prove that the situation presents a low risk. If sub-criterion c) is met, sub-criterion a) is broadly met and sub-criterion b) is not met.

101. *Criterion 10.15* – FIs are not permitted to carry out monetary operations until the customer identification process is complete (Art. 9(5) of the AML/CFT Law).

102. *Criterion 10.16* – The AML/CFT Law requires keeping CDD information on the customers up-to-date and reviewing them periodically. The AML/CFT guidelines for FIs stipulate that the CDD information renewal process shall be carried out following the RBA.

103. *Criterion 10.17* – According to Art. 14 AML/CFT Law, ECDD shall be carried out in several pre-defined high-risk situations (cross-border correspondent banking relationships; PEPs; customers from high-risk third countries). In addition, ECDD shall be applied where a higher risk of ML and/or FT is identified based on the FIs' risk assessment and management procedures.

104. *Criterion 10.18* – Art. 15(1) of the AML/CFT Law provides that simplified CDD may be carried out where a lower risk of ML and/or FT is identified based on the FIs' risk assessment and management procedures. Simplified CDD is limited to the cases indicated in the Law: *i.a.* companies traded on a regulated securities markets; entities of public administration; a FI covered by this Law, or registered in another EU Member State or in a third country which imposes requirements equivalent to those laid down in this Law and is supervised for compliance with those requirements; and certain life insurance contracts. Simplified CDD is prohibited in the cases where enhanced CDD is required (Art. 14), i.e. where a higher risk of ML/FT is identified. In cases of a suspicion of ML/FT full CDD must be carried out.

105. *Criterion 10.19* – FIs are prohibited from carrying out transactions through bank accounts, establishing or continuing business relationships and carrying out transactions when they are not in a position to complete the CDD requirements. In such cases, the FIs shall, upon assessment of the threat of ML and/or FT, decide on the appropriateness of forwarding a report on a suspicious monetary operation or transaction to the FCIS.

106. *Criterion 10.20* – Art. 9(22) of the AML/CFT Law provides that in case a FI has a suspicion that an act of ML and/or FT is carried out and further CDD may raise suspicion for the customer that information about him may be forwarded to the competent institutions, the FI may discontinue the CDD process and not establish a business relationship with the customer. In such cases, the information shall be forwarded to the FCIS.

Weighting and Conclusion

107. While most of the CDD measures put in place by the Lithuania meet the FATF Standards, minor deficiencies exist: The definition of monetary operations exempts payments to state and municipal institutions, other budgetary institutions, the BoL, state or municipal funds, foreign diplomatic missions or consular posts or settlement with these entities; The definition of customer excludes State and municipal institutions, other budgetary institutions, the BoL, state or municipal funds, foreign diplomatic missions or consular posts; There are no provisions related to the identification of representatives of legal arrangements; There are no obligations to understand the ownership or control structure of legal arrangements. The requested information for the identification of the

director of a legal person does not include the powers that regulate and bind the legal person; and the sub-criterion 10.14(b) is not met. **R.10 is rated LC**.

Recommendation 11 – Record-keeping

108. Lithuania was rated LC with former R.10 in the 2012 MER due to the absence of a requirement to maintain records of accounts' files and business correspondence; and of a provision to ensure that the record-keeping period may be extended in specific cases upon request of competent authorities.

109. *Criterion 11.1* – Requirements for the storage of information are defined in Art. 19(9-10) AML/CTF law. In particular, FIs must store data of the register for eight years from the date of termination of transactions or business relationships with the customer. The rules for the keeping of registers are established by the director of the FCIS; data kept in registers contains, as a minimum, identification data of the customer and BO, transaction amounts, dates, etc. FIs must store documents related to monetary operations for eight years from the date of execution of the monetary operation or conclusion of the transaction. The information storage period may be additionally extended for up to two years upon request a competent institution.

110. *Criterion 11.2* – Art. 19(10), (11) and (13) of the AML/CFT Law states that FIs must store copies of the identity documents of the customer, the BO and beneficiary as well as other documents obtained at the time of establishing the identity of the customer for eight years from the date of termination of transactions or business relationships with the customer. Business correspondence with the customer must be stored in paper or electronic form for five years from the date of termination of transactions or business relationships with the customer (Art. 19 AML/CFT Law). Art. 19(17) for analysis undertaken.

111. *Criterion 11.3* – Art. 19(12) is wide enough to include this requirement.

112. *Criterion 11.4* – The AML/CFT guidelines require FIs to ensure that all CDD information and transaction records are available swiftly to competent authorities upon appropriate authority.

Weighting and Conclusion

113. All criteria are met. **R.11 is rated C**.

Recommendation 12 – Politically exposed persons

114. Lithuania was rated LC with former R.6 in the 2012 MER. The shortcomings identified were the fact that the definition of PEPs did not cover all categories of senior government officials and excluded Lithuanian citizens entrusted with prominent public functions abroad; the lack of an explicit requirement to obtain senior management approval to continue the business relationship if the customer subsequently becomes a PEP; and effectiveness concerns.

115. *Criterion 12.1* – ECDD measures must be taken in case of transactions or business relationships with PEPs. The AML/CFT Law does not distinguish between domestic and foreign PEPs. Art. 2 (18) defines PEPs as natural persons who are or have been entrusted with prominent public functions and their immediate family members or close associates. All categories defined by the FATF Glossary are covered. Art. 14(3) of the AML/CFT Law provides that when carrying out ECDD, where transactions or business relationships are carried out with PEPs, FIs must identify and have in place internal procedures to determine whether the customer and the BO are PEPs. In addition, in case of PEPs, the

FIs must: obtain approval from a senior manager for establishing or continuing business relationships with such customers or continuing business relationships with the customers when they become PEPs; take adequate measures to establish the source of wealth[81] and source of funds that are involved in the business relationship or transaction (which include both customer and BO) and perform enhanced on-going monitoring of the business relationships.

116. *Criterion 12.2* – The same measures apply in relation to domestic PEPs and to persons entrusted with prominent functions in international organisations (cf. AML/CFT Law Art. 2 (18 & 19).

117. *Criterion 12.3* – The definition of PEPs includes *"immediate family members or close associates"*, as defined in Art. 2 AML/CFT Law. The requirements described under c.12.1 apply.

118. *Criterion 12.4* – Art. 14(7) of the AML/CFT Law refers to FIs involved in life insurance activities. Where the beneficiary or the BO is a PEP and where a higher risk of ML and/or FT is identified, the FIs shall, before pay-out: inform a senior manager of the future pay-out; perform enhanced monitoring of the monetary operations or transactions carried out by the customer or the beneficiary; and decide on the appropriateness of reporting a suspicious monetary operation or transaction to the FCIS. Those obligations are limited to ECDD measures and do not apply in all cases.

Weighting and Conclusion

119. All criteria are met. **R.12 is rated C**.

Recommendation 13 – Correspondent banking

120. Lithuania was rated C with former R.7 in the 2006 MER, hence it was not subject to re-evaluation in the course of the 4th round.

121. *Criterion 13.1* – According to Art. 14 of the AML/CFT Law, ECDD shall be carried out by applying additional measures of customer and BO identification where cross-border correspondent banking relationships are carried out with third-country FIs. Correspondent banking relationships within the EEA are not treated as cross-border, which is a deficiency. The definition of "Correspondent relationship" covers the provision of banking services and relationships between FIs where similar services are provided by a correspondent institution to a respondent institution, and including relationships established for securities transactions or funds transfers. For cross-border correspondent banking relationships, FIs should:

a) gather sufficient information about the respondent institution to fully understand the nature of its business and to determine from publicly-available information the reputation of the institution and the quality of supervision. There is no requirement to gather information on whether the respondent has been subject to an ML/FT investigation and regulatory action; b) assess control mechanisms for AML and/or CFT of the FI receiving funds; c) obtain approval from a senior manager before establishing new correspondent banking relationships; and d) document the respective responsibilities of each FI.

122. *Criterion 13.2* – Art. 14(2) 5) of the AML/CFT Law requires correspondent banks to be satisfied that the respondent institution has carried out proper identification of the customer (including

[81] The word « property » is indicated in the English translation of the AML/CFT Law but the Lithuanian version of the AML/CFT Law use the word « turtas » which means « wealth ».

verification of the identity of the customers having direct access to accounts of the correspondent institution and performance of other CDD actions) and that it is able to provide the relevant customer identification data to the correspondent institution upon its request.

123. *Criterion 13.3* – FIs are prohibited from establishing and continuing a correspondent banking relationship or any other relationships with a shell bank or a bank that is known to permit its accounts to be used by a shell bank. FIs must take measures to ascertain that the FIs receiving funds do not permit their accounts to be used by shell banks (Art. 14(8) AML/CFT Law).

Weighting and Conclusion

124. Correspondent banking relationships within the EEA are not treated as cross-border. However, specific information on this issue was provided by the Lithuanian authorities who confirmed that limited business is conducted with respondent institutions within the EEA. This deficiency is therefore given less weight. **R.13 is rated LC**.

Recommendation 14 – Money or value transfer services

125. Lithuania was rated LC with former SR.VI in the 2006 MER due to insufficient control on money transfer services provided by the Post Office. No re-evaluation was done in the 4th round.

126. *Criterion 14.1* – MVTS comprise payment service providers (PSPs), credit institutions, payment institutions (PIs) and electronic money institutions (EMIs) (Art. 6 of Law on Payments). The authorities indicate that the definition of MVTS in the FATF Recommendations is similar to the scope of activities that PIs and EMIs are licensed to carry out. Both categories are subject to licensing by the BoL. According to Art. 7(2) of Law on Payments, PSPs mentioned in Art. 6(4), (5) and (6) may provide payment services without a license. This exemption comes from the Payment Services Directive and applies to the Post in relation to post transfers. Art. 7 of the Law on Payments prohibits natural or legal persons that are not PSPs to carry out payment services listed in Art. 5 of the Law.

127. *Criterion 14.2* – Persons carrying out MVTS without a licence or registration can be identified by initiative of the supervisors (while monitoring the market, assessing the types of services provided or complaints made by consumers, etc.). Art. 66 of the Law on Payments *"allows to apply sanctions to natural persons that practice commercial or professional activity, and to legal persons when they conduct operations or activity prohibited by this Law"*. A warning may be issued after the BoL makes an investigation of that person's activities. A warning would serve as a "soft" penalty (if circumstances allow). If, as a result of the investigation severe or repeated infringements of the Law are established, the BoL may issue a fine (up to 2% of the annual income for legal persons; up to EUR 50,000 for natural persons that carry out a commercial or professional activity).

128. *Criterion 14.3* – According to Art. 4 AML/CFT Law, the BoL shall approve instructions aimed at preventing ML and/or FT intended for *(i.a.)* EMIs and PIs. The BoL shall supervise the activities of these entities related to the implementation of ML and/or FT prevention measures and give advice to these entities on the issues relating to the implementation of the instructions specified in this paragraph. The FIU monitors the Post Office in relation to post office transfers.

129. *Criterion 14.4* – PSPs wishing to operate through an agent must apply to the BoL to have the agent added to the public list of PIs or EMIs. Once registered, the agent may start providing payment services on behalf of the PSP. The list of the PSPs' agents is maintained by the BoL. Unauthorised

agents of a PI or EMI cannot operate in Lithuania. An agent registered in another country can operate in Lithuania if the BoL receives notification from a supervisor of the country (if the agent is a registered agent of a PI or EMI licenced by a supervisor of another EU member state).

130. *Criterion 14.5* – Art. 16 of the Law on Payment Institutions includes the obligation for MVTS providers to include their agents in their AML/CFT programmes and monitor them for compliance with these programmes.

Weighting and Conclusion

131. All criteria are met except for criterion 14.1. PSPs mentioned in Art. 6(4), (5) and (6) (the Post) may provide payment services without a license. **R.14 is rated LC**.

Recommendation 15 – New technologies

132. Lithuania was rated LC with former R.8 in the 2006 MER due to deficiencies in the non-banking financial sector. No re-evaluation was done in the 4th round.

133. *Criterion 15.1* – As per Art. 14(10) of the AML/CFT Law, when identifying whether there is a higher risk of ML and/or FT, FIs must assess amongst other risk factors, products, service, transaction or delivery channel risk, including whether new or developing technologies are used for both new and existing products. In addition, Art. 55 of the AML/CFT Guidelines for FIs provide that financial market participants must assess the ML and/or FT risks related to the implementation of new services and products, the use of new (developing) technologies in business. There are no legal requirements for the country to undertake such a risk assessment but the Lithuanian authorities (most notably the BoL and the FIU) have taken numerous actions in order to identify and assess the related risks. That resulted in the issuance of recommendations, positions and warnings regarding risks linked to the use of certain products, services and business practices, the introduction of different risk mitigating measures, the drafting of amendments to the AML/CFT Law aiming to regulate new products or services, which prove that risks mentioned under this criterion are being identified and assessed at the national level.

134. *Criterion 15.2* – Art. 55 of the AML/CFT Guidelines for FIs requires that FIs should carry out a risk assessment before starting to provide new services or offering new products or intending to use the new (developing) technologies. Based on the findings (results) of such an assessment, respective measures shall be taken in order to minimize the risks.

Weighting and Conclusion

135. All criteria are met. **R.15 is rated C**.

Recommendation 16 – Wire transfers

136. Lithuania was rated LC with former SR.VII in the 2012 MER. The evaluators noted that there was no explicit provision to determine the competent authorities and to establish the appropriate monitoring, enforcement and penalties regime.

137. *Criterion 16.1* – Art. 9(1)(5) of the AML/CFT Law provides that FIs must identify and verify the identity of customers and BOs when executing and accepting money transfers, in accordance with EU Reg. 847/2015. Art. 4 of the Regulation covers all elements of c.16.1.

138. *Criterion 16.2* – C.16.2 on batch files is implemented through Art. 6, 7(2) and 11(2)c) of EU Reg. 847/2015, with relevant references to Art. 4 for required and accurate originator information, as well as for required beneficiary information.

139. *Criterion 16.3* – Under Art. 6 of the EU Reg. 847/2015, cross-border wire transfers below EUR 1,000 should always be accompanied by the required originator and beneficiary information.

140. *Criterion 16.4* – According to Art. 6 of the EU Reg. 847/2015, FIs need not verify the information on the originator unless, inter alia, they have reasonable grounds for suspecting ML/FT.

141. *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 Standards. Art. 5 of the EU Reg. 847/2015 prescribes that such transfers shall be accompanied by at least the payment account number of both the originator and the beneficiary, or by the unique transaction identifier. There is a 3 working day period established for the ordering FI to make available required originator information whenever requested to do so by the beneficiary or intermediary FI. In addition, Art. 14 of EU Reg. 847/2015 requires FIs to respond fully and without delay to enquiries from appropriate AML/CFT authorities.

142. *Criterion 16.7* – Art. 16 of the EU Reg. 847/2015 establishes a 5 year period for FIs to maintain records of originator and beneficiary. Upon expiry of this period, personal data is to be deleted, unless provided for otherwise by national law. The Regulation allows Member States to decide upon further retention only after carrying out a thorough assessment of the necessity and proportionality of such further retention, and where it is justified for the ML/FT purposes. That further retention period shall not exceed five years.

143. *Criterion 16.8* – The EU Reg. 847/2015 (Art. 4) prohibits the ordering FI to execute any transfer of funds before ensuring full compliance with its obligations concerning the information accompanying transfers of funds.

144. *Criterion 16.9* – Art. 10 of the EU Reg. 847/2015 requires intermediary FIs to ensure that all the information received on the originator and the beneficiary accompanying a transfer of funds is retained with the transfer.

145. *Criterion 16.10* – The EU Reg. 847/2015 does not provide for the exemption specified in this criterion regarding technical limitations preventing the appropriate implementation of the requirements on domestic wire transfers.

146. *Criterion 16.11* – Art. 11 of the EU Reg. 847/2015 obliges the intermediary FI to implement effective procedures including, where appropriate, ex-post or real-time monitoring, in order to detect whether required originator or beneficiary information in a transfer of funds is missing.

147. *Criterion 16.12* – The intermediary FI should have effective risk-based procedures for determining whether to execute, reject or suspend a transfer of funds lacking the required payer and payee information and for taking the appropriate follow up action (Art. 12 of the EU Reg. 847/2015). If the service provider has not been provided with the required payer or payee data, it shall reject the transfer or ask for the required information on the payer and the payee before or after the transmission of the transfer of funds, on a risk-sensitive basis.

148. *Criterion 16.13* – According to Art. 7 of the EU Reg. 847/2015, the obliged entity of the beneficiary shall implement effective procedures, including, where appropriate, ex-post monitoring or real-time monitoring, in order to detect whether information on the payer or the payee is missing for transfers of funds where the PSP of the payer is established outside the EU, as well as for batch file transfers where the PSP of the payer is established outside the EU.

149. *Criterion 16.14* – Art. 7 of the EU Reg. 847/2015 provides that, in the case of transfers of funds exceeding EUR 1,000, the beneficiary FI shall verify the accuracy of the identification information on the beneficiaries before crediting their payment account or making the funds available to them.

150. *Criterion 16.15* – Art. 8 of the EU Reg. 847/2015 obliges the beneficiary FI 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.

151. *Criterion 16.16* – This criterion is met except in relation to post transfers.

152. *Criterion 16.17* – When a PSP holds information concerning both the originator and the beneficiary, it must take all of this information into account as part of its due diligence process, with a view to determining whether the transaction should be considered 'unusual' and suspicious, and therefore reported to the FIU.

153. *Criterion 16.18* – FIs that conduct wire transfers are subject to the domestic and EU requirements that give effect to UNSCRs 1267 and 1373, and successor resolutions.

Weighting and Conclusion

154. Post transfers are not subject to the requirements stemming from C.16.16. **R.16 is rated LC**.

Recommendation 17 – Reliance on third parties

155. Lithuania was rated LC with former R.9 in the 2006 MER due to deficiencies in the definition of third parties and introducers. No re-evaluation was done in the course of the 4th round.

156. *Criterion 17.1* – "Third party" is defined in Art. 2(21) of the AML/CFT Law as a FI or another obliged entity in Lithuania or the EU (registered in another EU Member State) or a third country (a state that is not a Member State of the European Union) meeting the following requirements: 1) subject to mandatory professional registration prescribed by law; 2) registered in a EU Member State or a third country which imposes requirements equivalent to those established by the EU for the identification of the customer and of the beneficial owner and storage of information and they are supervised for compliance with those requirements.

157. Art. 13 prescribes that the responsibility for compliance with the CDD requirements rests with the FIs that have used information from a third party. When establishing the identity of the customer or the BO, FIs may use information from third parties, provided that they have sufficient means to ensure that the third party will voluntarily comply with both of the following conditions: 1) it will, upon request, immediately provide to the requesting FI or another obliged entity all information and data required to be held in compliance with the CDD requirements laid down in the Law; and 2) it will, upon request, immediately provide to the requesting FI or another obliged entity copies of the documents relating to identification of the customer or of the BO and other documents relating to the

customer or the BO which are required to be held in compliance with the CDD requirements laid down in the Law. Condition c of c.17.1 is included in the definition of third party i.e. Art 2(21).

158. *Criterion 17.2* – Art. 13(1) and (3) of the AML/CFT Law cover this requirement. Additionally, the AML/CFT guidelines for FIs (Art. 15) provide that the financial market participants are required to satisfy themselves that the third party complies with the AML/CFT Law requirements, taking into account the information about ML and FT risks in the third party's country of registration.

159. *Criterion 17.3* – Art. 13 does not distinguish between reliance on an entity within the group or an entity which is a third party.

Weighting and Conclusion

160. All criteria are met. **R.17 is rated C**.

Recommendation 18 – Internal controls and foreign branches and subsidiaries

161. Lithuania was rated LC with former R.22 in the 2012 MER, due to deficiencies identified in the insurance sector. For former R.15, Lithuania was rated LC in the 2006 MER (there was no obligation for FIs to develop CFT internal controls programs), which was not re-evaluated in the 4th round.

162. *Criterion 18.1* – According to Art. 22(1) of the AML/CFT Law FIs are required to designate senior employees for organising the implementation of AML/CFT prevention measures. Where obliged entities are led by a board, one member must be in charge with AML/CFT matters. Art. 60(4) of the AML/CFT guidelines for FIs provides that the management of financial market participants must ensure that the ML and FT prevention measures are properly integrated into the internal control system (including vetting of persons being employed, audit of their activities). Furthermore, AML/CFT preventive measures shall include the participation of the relevant employees in special on-going AML/CFT training programmes aiming to help employees to recognise suspicious operations which may be related to ML and/or FT (Art. 22(2) AML/CFT Law).

163. *Criterion 18.2* – As per Art. 22 (3) of the AML/CFT Law, FIs that are part of a group must implement the group-wide policies and procedures for the prevention of ML and/or FT, and comply with the national legislation of the EU Member State in which the subsidiary or branch is established (including confidentiality requirements). Art. 23(1) (4) allows for disclosure between FIs registered in the EU Member States or in third countries which are subject to requirements equivalent to those laid down in the AML/CFT Law, provided that these entities are part of one group. It is unclear what type of information is allowed for "disclosure". There is no requirement on the provision of group-level compliance, audit, and/or AML/CFT functions, of customer, account, and transaction information from branches, if necessary.

164. *Criterion 18.3* – Where legal AML/CFT provisions of Lithuania differ from those of a foreign state, branches or majority-owned subsidiaries must apply the stricter provisions in so far as the legislation of the foreign state so permits. Where the legislation of the foreign state does not permit the application of requirements equivalent to international ones, the FIs must immediately inform the FCIS thereof and, having agreed with it, take additional measures to effectively reduce the risk of ML and/or FT. Where these additional measures are insufficient for reducing such risk, FIs must refuse to enter into or discontinue monetary operations or transactions and business relationships with the customer or cease activities in a third country (Art. 22(4) AML/CFT Law).

Weighting and Conclusion

165. There is no requirement on the provision of group-level compliance, audit, and/or AML/CFT functions, of customer, account, and transaction information from branches, if necessary. **R.18 is rated LC**.

Recommendation 19 – Higher-risk countries

166. Lithuania was rated LC with former R.21 in 2006 MER due to provisions limited to the customers of banking institutions. Lithuania was not re-evaluated in the course of the fourth round.

167. *Criterion 19.1* – As per Art. 14 of the AML/CFT Law, ECDD shall be carried out where transactions or business relationships are carried out with legal and natural persons established in high-risk third countries included in lists of jurisdictions with strategic deficiencies in their AML/CFT systems as published by the EC and the FATF. ECDD measure might include: obtaining approval from a senior manager for establishing or continuing business relationships with such customers; take adequate measures to establish the source of property and source of funds that are involved in the business relationships or transaction; or perform enhanced on-going monitoring of the business relationships. When identifying whether there is higher risk of ML and/or FT, FIs must assess a number of risk factors, including high-risk jurisdictions.

168. *Criterion 19.2* – There is no specific provision in the AML/CFT Law on countermeasures. Art. 14 of the AML/CFT Law does not contain a sufficient range of measures (only ECDD). On that basis Lithuania cannot apply countermeasures independently of any call by the FATF (or the EC).

169. *Criterion 19.3* – The FCIS circulates the lists of countries identified by the FATF and the lists are posted on the FCIS's website.

Weighting and Conclusion

170. There is not specific provision in the AML/CFT on countermeasures. Art. 14 of the AML/CFT Law does not contain a sufficient range of measures (only ECDD). **R.19 is rated LC**.

Recommendation 20 – Reporting of suspicious transaction

171. Lithuania was rated PC with former R.13 in the 2012 MER, as the reporting regime was not based on a suspicion that the funds are proceeds of crime, but that they constitute ML; the complex reporting arrangements carried risks of inconsistencies; and there were serious effectiveness issues.

172. *Criterion 20.1* – FIs must immediately, no later than within one working day, report to the FIU if they know or suspect that property of any value is, directly or indirectly, derived from a criminal act or from involvement in such an act, or know or suspect that such property is used to support one or several terrorists or a terrorist organisation. This wording limits the reporting in case of FT to "support" of terrorists or terrorist organisations, and it is more restrictive than the Standard which refers to "FT" in general.

173. *Criterion 20.2* – As per Art. 16 of the AML/CFT Law, upon receipt of the information that the customer intends or will attempt to carry out a suspicious monetary operation or transaction, FIs must immediately notify the FCIS. Suspicions related to property of any value must be reported.

Weighting and Conclusion

174. The wording in Art. 16(1) of the AML/CFT, "support" of terrorists or terrorist organisations, is more restrictive than the Standard which refers to "FT" in general. **R.20 is rated LC**.

Recommendation 21 – Tipping-off and confidentiality

175. Lithuania was rated LC with former R.14 in the 2006 MER due to the lack of adequate protection when reporting. Lithuania was not re-evaluated in the course of the fourth round.

176. *Criterion 21.1* – As per Art. 16(13) of the AML/CFT Law, FIs shall not be responsible to the customer for the non-fulfilment of contractual obligations and for the damage caused by suspicious transactions reporting. Immunity from legal proceedings shall also apply to directors or other employees of FIs who report, in good faith, information about suspected ML or FT or suspicious monetary operations or transactions to the responsible employees at their workplace or to the FCIS. They may not be subject to disciplinary sanctions because of such actions.

177. *Criterion 21.2* – Supervisors, obliged entities and their employees are prohibited from notifying the customer or other persons that the information has been submitted to the FCIS or any other supervisor (Art. 23(3) of the AML/CFT law).

Weighting and Conclusion

178. All criteria are met. **R.21 is rated C**.

Recommendation 22 – DNFBPs: Customer due diligence

179. Lithuania was rated PC with former R.12 in the 2012MER for deficiencies identified in R.5, 6, 10 and 11, which equally applied to DNFBPs.

180. *Criterion 22.1* – According to the AML/CFT Law, the identification requirements described under R.10 apply to "FIs" and "other obliged entities". According to Art. 2(10), "Other obliged entities" means: gaming companies and lottery companies (in all cases); real estate agents and brokers; persons engaged in commercial activities involving trade in precious stones and metals or any other property of EUR 10,000 or more when the payment is made in cash; lawyers, notaries and accountants in cases mentioned by C.22.1 (Requirement on buying and selling of business entities is missing) and providers of trust or company incorporation or administration services. "Other independent legal professions" as listed by R.22 are not covered by the AML/CFT Law.

181. *Criterion 22.2* – DNFBPs must comply with all record-keeping obligations applying to FIs.

182. *Criterion 22.3* – The AML/CFT Law applies equally to FIs and DNFBPs in respect of PEPs.

183. *Criterion 22.4* – As with FIs, when identifying whether there is higher risk of ML and/or FT, obliged entities must assess, among other risk factors, product, service, transaction or delivery channel risk, including assessment whether new or developing technologies are used for both new and pre-existing products.

184. *Criterion 22.5* – The AML/CFT Law applies equally to FIs and DNFBPs (see R.17).

Weighting and Conclusion

185. The requirement for lawyers, notaries, other independent legal professions and accountants to comply with the CDD requirements set out in R.10 is not covered in relation to buying and selling of business entities. **R.22 is rated LC**.

Recommendation 23 – DNFBPs: Other measures

186. Lithuania was rated PC with former R.16 in the 2012 MER due to gaps in the STR system and insufficient provisions relating to internal control procedures and independent audit functions.

187. *Criterion 23.1* – The same requirements apply for DNFBPs and FIs as regards STRs, except for notaries, notary's agents and persons entitled to perform notarial actions, auditors, judicial officers and judicial officer's agents, undertakings providing accounting or tax advisory services in the course of ascertaining the legal position of their client, or representing that client in criminal, administrative or civil proceedings, including advice on instituting or avoiding proceedings. The obligation does not apply either to advocates and advocates' assistants in the course of ascertaining the legal position of their client or defending or representing the client in, or concerning judicial proceedings, including advice on instituting or avoiding proceedings, irrespective of whether such information is received or acquired prior to, in the course of or upon termination of such proceedings. This is in line with the FATF requirements.

188. *Criterion 23.2* – The same requirements apply to FIs and DNFBPs (see R.18).

189. *Criterion 23.3* – The same requirements apply to FIs and DNFBPs (see R.19).

190. *Criterion 23.4* – The same requirements apply to FIs and DNFBPs (see R.21).

Weighting and Conclusion

191. Minor deficiencies in relation to R.18, R.19 and R.20 are equally relevant to DNFBPs. **R.23 is rated LC**.

Recommendation 24 – Transparency and beneficial ownership of legal persons

192. Lithuania was rated Partially Compliant with the former R.33. The 4th round evaluation noted that although some positive measures for the communication of shareholders for limited liability companies had been put in place, it remained unclear whether the Register kept information on the ownership/shareholder for all relevant forms of legal entities. Furthermore, information on ownership was not available systematically in electronic form whilst the level of penalties for non or false declaration was low. The assessors also raised concerns with regard to the fact that service providers were used as front-structures in practice.

193. *Criterion 24.1* –

a) Types, forms and basic features of legal persons - The Second Book, Part II Legal Persons, Chapter IV General Provisions of the Civil Code and Regulations of the Register of Legal Entities approved by Resolution No. 1407 of the Government of the Republic of Lithuania, dated 12 November 2003 provides information on the different types and forms of legal persons that can be established in the country.

Article 2.34 of the Civil Code stipulates that legal persons in Lithuania are divided in public and private legal persons. Moreover, the Civil Code stipulates that religious communities and associations

(Article 2.37) and Trade Unions (Article 2.38) are considered as well as legal persons. Basic provisions for legal persons are provided in the Civil Code, in the Law on Companies and in Laws regulating specific legal forms of legal persons.

b) Processes for creation of legal entities and obtaining information - Article 2.59 of the Civil Code requires legal persons to be incorporated pursuant to the procedure established by the law and the Civil Code. Moreover, Art. 2.62 of the Civil Code stipulates that legal persons have to be registered with the RLE and Art. 2.64 lists the documents which must be produced to the RLE. The Law on Companies and other laws regulating the specific legal form of legal persons indicate the requirements in order to create the different types of legal persons. The website of the Register provides guidance on this point.

Basic information on each type of legal entity incorporated in Lithuania is available on the website of the RLE. The RLE contains complete information (and historical data) about legal form and status of legal entities, fields of their activity, size and structure of the authorised capital, members of sole and collective management bodies, licenses acquired, etc. Excerpts from the Register on any legal entity stored in the archive of the Register are accessible for anybody for a fee set by the Government.

There is no direct data available with regard to the beneficial owners of the different types of Lithuanian legal persons but information can be obtained regarding shareholders of different types of legal persons:

- The Register of Legal Entities provides publicly available information for single shareholder companies;

- In case of multiple shareholders, the Information System of Members of Legal Entities JADIS provides information with regard to the most common types of legal persons (private limited companies, public institutions, small communities).

Information on shareholders, owners, members of some types of legal persons is not available.

194. *Criterion 24.2* – Lithuania did not assess the ML/FT risks posed by the different types of legal persons that can be created in the country.

195. *Criterion 24.3* – Article 2.62 of the Civil Code imposes an obligation to all legal entities to be registered (see c.24.1.b). Article 2.66 of the Civil Code lists the data the Register of legal Entities has to include: 1) company name; 2) legal form; 3) code; 4) registered office address; 5) bodies of the legal person; 6) managing bodies and their members (name, surname, personal code, place of residence); 7) members of managing bodies and members of a legal person who have the right to conclude contracts on behalf of the legal person, power of signature; 8) branch offices and representative offices ; 9) restrictions on the activities; 10) legal status; 11) expiry of the term; 12) dates of alterations in the data filed with the register and dates of the alteration of documents; 13) financial year and other data prescribed by the law. Register data, documents and all other information submitted are public (Art. 2.71 and 2.72 of the Civil Code).

196. *Criterion 24.4* – No information has been provided to the evaluation team on this criterion.

197. *Criterion 24.5* – Art 2.66(2) of the Civil Code imposes an obligation on legal entities, in cases when the registered data, documents submitted in the registration process or any other data have changed or have been changed, to submit the new data and request the registration of the changes with the Register of Legal Entities within thirty days as of the day these changes were made. The afore-mentioned submission of new/changed data has to be done in the specific form developed by

the Register for such purposes. As regard to shareholder information, this only applies to some legal persons.

198. Under Art 2.67 of the Civil Code managing body of a legal person shall be responsible for the timely production of documents of a natural person, data and other requested information to the Register of Legal Entities except as otherwise provided by the law or incorporation documents.

199. As per the Law on Administrative Offences (Art. 589 and 223) the Register has the right to initiate administrative proceedings against the responsible person of the legal entity (management body) for failure to submit new data or for submitting inaccurate data to the Register.

200. There is no Authority responsible for verifying updates of information submitted to the Register by legal persons.

Beneficial Ownership Information

201. *Criterion 24.6* – In order to obtain information on the beneficial ownership of a company, the authorities mainly rely on existing data held by banks in accordance with Recommendation 10. Thus the information on the BO can easily be determined by the Financial Crime Investigation Service, which, through the banks, has a right of access provided by the AML/CFT Law.

202. Article 25 of the AML/CFT Law, which will enter into force on 1 January 2019, stipulates that all legal entities founded in Lithuania, except for those whose sole member is the state or a municipality, must obtain, update and store accurate information on their BOs or on other rights of control (the chair of the board, board member, director, senior manager, other position and the number of transferred voting rights expressed through a percentage). The same article provides that such information must be submitted (no later than ten days from the date the data has been changed) to the manager of JADIS in accordance with the procedure laid down in the regulations for this information system. Specified information on the BOs must be submitted to the manager of JADIS until 1 July 2019[82].

203. *Criterion 24.7* – As stated in C. 24.6, the mechanism to ensure availability of BO information relies on existing data held by banks in accordance with Recommendation 10. Article 9 (17) of the AML/CFT Law requires banks to review and keep up-to-date documents, data and information submitted by the customer and the beneficial owner when applying CDD.

204. *Criterion 24.8* –

a) There are no requirements in the Civil Code or in the Laws on Companies for an individual to be authorised as the accountable person to provide the authorities with basic and BO information and to give further assistance.

b) There are no requirements in the Civil Code or in the Laws on Companies for a DNFBP to be authorised as the accountable person to provide the authorities with basic and BO information and to give further assistance.

[82] From the second half of 2019, the Authorities will use this mechanism to ensure that information on the beneficial ownership of a company is available. This will increase further the efficiency in terms of BO determination. These provisions have not been considered for conclusions or rating as they were not in force and effect at the time of onsite.

c) The authorities did not provide information on any other comparable measures identified by the country in order to cooperate with competent authorities to the fullest extent possible in determining the beneficial owner.

205. *Criterion 24.9* – The Regulations of the Register of Legal Entities (Paragraph 136) state that when a legal entity ceases to exist all data stored in the Register concerning this entity are transferred to the Register's archive and stored for a period of 50 years. Article 19 (9) of the AML/CFT Law requires banks to store register data from their customers and BOs for eight years from the date of termination of transactions or business relationship with the customer. It is not clear how long legal persons are required to retain basic and beneficial ownership information.

206. *Criterion 24.10* – As noted under C.24.1.b, data, documents and all other information submitted to the JADIS are available to state institutions to implement their functions. Information submitted to the Register of Legal Entities is public and thus also available to law enforcement authorities. Information with regard to the beneficial ownership of legal persons can be obtained from banks by the Financial Crime Investigation Service (Article 7 (1) of the AML/CFT Law).

207. *Criterion 24.11* –Article 40(2) of the Lithuanian Law on Companies states that all shares in companies shall be registered. The Law on Banks (Art. 41(2)) prohibits bank issuing bearer shares. As only companies can issue shares in Lithuania, all shares shall be registered.

208. *Criterion 24.12* – No mechanisms are in place in Lithuania in order to ensure that nominee shares and nominee directors are not misused for ML/FT. However, the use of nominee shares and nominee directors is not a widespread practice in Lithuania.

209. *Criterion 24.13* – Paragraph 1 of Article 223 of the Code of Administrative Offences provides that failure to meet the requirements on timely submission or submission of false data, documents or other requested information to the Register or to the JADIS are subject to fines ranging from EUR 30 to 1,450. Fines may be imposed to the directors of legal entities, directors of their branches or representative offices, directors of the branches or representative offices of the foreign legal entities or other organisations or persons referred to in the relevant laws or legal entities foundation documents/statutes. The range of the monetary fine is neither proportionate nor dissuasive. Moreover, the Centre of Register indicated that no sanctions have been applied yet in cases foreseen by the law.

210. Article 9 (1) of the AML/CFT Law requires banks to identify and verify the identity of the beneficial owners of their clients. The Bank of Lithuania is able to impose sanctions to banks in case of failure to comply with these requirements. Nevertheless, the BoL has advised the evaluation team that no sanctions have been imposed against FIs in relation to inadequate identification or verification of BOs.

211. *Criterion 24.14* – Lithuania can rapidly provide international cooperation in relation to basic and beneficial ownership information: (a) Lithuania can facilitate access to basic information held by the Register of Legal Entities. Foreign authorities can freely access basic information via the online Register of Legal Entities website; (b) authorities can rapidly exchange information on shareholders as set out in Recommendations 37 and 40; (c) beneficial ownership information provided by the legal person can be obtained via a request to the FIU, without need for engagement with Lithuanian authorities or resort to investigative powers.

212. *Criterion 24.15* – Lithuania does not have any mechanism in place which would monitor the quality of assistance rendered from other countries and related to exchange of BO information.

Weighting and Conclusion

213. There is a number of deficiencies in relation to the transparency and beneficial ownership of legal persons: There is no direct data available with regard to the beneficial owners of the different types of Lithuanian legal persons; JADIS does not contain information on shareholders of some types of legal persons; Lithuania did not assess the ML/FT risks posed by the different types of legal persons that can be created in the country; No information has been provided to the evaluation team on C.24.4; There is no Authority responsible for verifying updates of information submitted to the Register by legal persons; The requirement under C.24.5 in relation to shareholder information applies only to some legal persons; C24.8 is not met; It is not clear how long legal persons are required to retain basic and beneficial ownership information; There are no mechanisms in place to ensure that nominee shares and nominee directors are not misused for ML/FT; The range of the monetary fine is neither proportionate nor dissuasive; The Centre of Registers indicated that no sanctions have been applied yet in cases foreseen by the law; and Lithuania does not have any mechanism in place which would monitor the quality of assistance rendered from other countries and related to exchange of BO information. **R.24 is rated PC.**

Recommendation 25 – Transparency and beneficial ownership of legal arrangements

214. In the 2012 MER, former R.34 was considered Non-Applicable - the concept of trusts or other legal arrangements was not known under the laws of Lithuania.

215. *Criterion 25.1* – Lithuania is not a signatory to the Hague Convention on Laws Applicable to Trusts and their Recognition. There are no trusts governed under the laws of Lithuania. (a) and (b) do not apply. With respect to (c), the AML/CFT Law defines a trust or company incorporation and administration service provider as any natural or legal person which, inter alia, provides the following service: acting as, or arranging for another person to act as, a trustee of an express trust or a similar legal arrangement. A trustee in Lithuania of a trust governed under the laws of another country must comply with record keeping obligations including the information referred to in (a) and (b).

216. *Criterion 25.2* – Art. 25 (see c.25.1) read in conjunction with Art. 14 and 15 of the AML/CFT Law clearly require that any information is kept accurate, up to date and updated on a timely basis.

217. *Criterion 25.3* – Authorities advised that Art. 12(2) of the AML/CFT Law, which obliges obliged entities, when establishing the identity of the BO, and requiring the customer and the BO to provide the relevant identification data, to meet the requirements of this criterion. This provision does not require the disclosure of trustee status by the trustee himself to FIs or DNFBPs when forming a business relationship.

218. *Criterion 25.4* – There is nothing in any law in Lithuania that would prevent trustees from providing competent authorities with any information relating to the trust.

219. *Criterion 25.5* – The powers of competent authorities referred to under R.27, 29 and 31 apply in this case.

220. *Criterion 25.6* – There are no impediments to provide information to foreign partners.

221. *Criterion 25.7* – Trustees are subject to the sanctions envisaged under the AML/CFT Law.

222. *Criterion 25.8* – The authorities advised that Art. 223(1) of the Code of Administrative Offences foresees a fine ranging from EUR 30 to 1,450 for failure to meet the requirements on timely submission or for the submission of false data, documents and other requested information to the RLE or JADIS. Given the definition in Art. 2(14) AML/CFT Law, trusts are covered by these provisions. The range of the monetary fine is neither proportionate nor dissuasive.

Weighting and Conclusion

223. Lithuania has no measures in place to ensure that trustees disclose their status to FIs and DNFBPs when forming a business relationship above the threshold or carrying out an occasional transaction. The range of the monetary fine available for legal arrangements is neither proportionate nor dissuasive when they fail to meet the requirements for timely submission or for submission of false data, documents and other requested information to the RLE and/or JADIS. **R.25 is rated LC**.

Recommendation 26 – Regulation and supervision of financial institutions

224. Lithuania was rated Largely Compliant with the former R.23. The then assessment team made several observations which were all related to effective supervision (e.g. lack of focused examinations, lack of risk-based approach in supervision, week supervision of insurance and security sectors) whilst no particular shortcoming was identified with regard to the legal framework.

225. *Criterion 26.1* – Under the Single Supervisory Mechanism (SSM) the European Central Bank (ECB) is responsible for the prudential supervision of significant banks. Both the AML/CFT Law (Art. 4(1)) and the Law on Banks (Art. 8(2)(2)) designate the BoL as responsible for AML/CFT regulation and supervision of financial institutions. In addition, the FIU has responsibilities under the AML/CFT Law (Art. 4(9)) for the AML/CFT supervision of all obliged entities; the operational responsibility of the BoL in practice is articulated in a cooperation agreement signed by the two authorities.

226. *Criterion 26.2* – The following statutory provisions provide for mandatory licensing by the BoL:

- Banks: Art. 9(1) and (3) of the Law on Banks. Regarding Core Principles FIs, Credit institutions are licensed by the European Central Bank (ECB), which cooperates with the BoL.
- Insurance: Art. 12(1) of the Law on Insurance;
- Credit unions: Art. 9 of the Law on Credit Unions of the Republic of Lithuania;
- Central credit union: Art. 9 of the Law on Central Credit Union of the Republic of Lithuania;
- Electronic money institutions. Articles 11 and 12 of the Law on Electronic Money and Electronic Money Institutions of the Republic of Lithuania;
- Payment institutions: Arts. 5 and 6 of the Law on Payment Institutions of the Republic of Lithuania;
- Consumer credit providers: Art. 22(1) of the Law on Consumer Credit of the Republic of Lithuania;
- P2P platforms: Art. 25^1(1) of the Law on Consumer Credit of the Republic of Lithuania;
- Investment companies:

a) Arts. 7 and 9 of the Law on Collective Investment Undertakings Intended for Informed Investors of the Republic of Lithuania;

b) Art. 5(1) of the Law on Collective Investment Subjects of the Republic of Lithuania;

- Management companies:

c) Arts. 7 and 9 of the Law on Collective Investment Undertakings Intended for Informed Investors of the Republic of Lithuania;

d) Art. 6(1) of the Law on Management Companies of Collective Investment Undertakings Intended for Professional Investors of the Republic of Lithuania;

e) Art. 5(1) of the Law on Collective Investment Subjects of the Republic of Lithuania;

- Crowdfunding platforms: Art. 6 (1) of the Law on Crowdfunding of the Republic of Lithuania;
- Financial brokerage companies and financial adviser companies: Article 4 (1) of the Law on Markets in Financial Instruments of the Republic of Lithuania;
- Currency exchange operators: Art. 11 of the Law on Currency Exchange Operators of the Republic of Lithuania;
- Credit providers when credit is related to real estate: Art. 25 of the Law on Real Estate Related Credit of the Republic of Lithuania;
- Financial institutions: Art 1 of the Law on Financial Institutions of the Republic of Lithuania.

227. Articles 3, 9, 10 and 30 onwards of the Law on Banks require a bank to have substance. The BoL can withdraw the licence of inactive banks under this law and Art. 10 of the Law on Financial Institutions where a bank is inactive. The provisions prevent the establishment and operation of shadow banks.

228. *Criterion 26.3* – The Law on Banks (Art. 25(1 and 8) and 34(2, 7, 8, 12 and 13)), sets out the regulatory measures to prevent persons with criminal records from holding a management function or being the legal owner or BO of a significant or controlling interest in a FI.

229. These provisions (Articles 25(8)(1), 34(12) and 34(13) are mutatis mutandis applied to the majority of other financial institutions and their management, shareholders and BOs. In some cases (some types of financial institutions), due to lower risk and lesser complexity of some of the financial institutions' activities, similar, although easier to fulfil, criteria are layed out in dedicated regulation of these financial institutions.

230. Managers, legal owners and beneficial owners must have an impeccable reputation. A person may not be regarded as being of good repute if he/she: i) has been convicted for a serious crime or for a crime against property, property rights and property interests, economy and business practice, the financial system or of corresponding criminal acts under criminal laws of foreign states, irrespective of whether the conviction has expired; ii) has been administratively or disciplinary sanctioned for infringement of laws or other legal acts regulating the provision of financial services and activities and where he/she has been sanctioned more than once during a year. The BOL can also conclude that a person is not of good reputation taking into consideration other criteria such as conviction for a crime other than those specified under i) above; if he/she acquires a qualifying

holding in the bank's authorised capital and/or voting rights, or if these increased, were transferred or reduced without giving notice beforehand to the supervisory authority, in cases where such notice is required; the imposition of sanctions or was involved in a winding up of a legal person by reason of bankruptcy or by a court's decision or judgement on other statutory grounds related to inappropriate activities or infringements of legal acts; and the suspension, while having a qualifying holding in a FI's authorised capital and/or voting rights, of his right to exercise the voting right at the general meeting of the FI's members.

231. Annexes to the Resolution of the Board of the Bank of Lithuania No 03-181 On the Approval of Guidelines on the Assessment of Members of the Management Body and Key Function Holders of the Financial Market Participants Supervised by the Bank of Lithuania and the Resolution of the Board of the BoL No.03-138 specify the level of information required in relation to banks.

232. Articles 24(1), 24(4) and 34(4) of the Law on Banks set a requirement for prior approval by the BoL in case of a change of management, legal owners and beneficial owners. The legislation in c.26.2 applies the same provisions to other FIs.

233. Under Art. 34 of the Law on Banks the BoL can consider that an associate of a criminal is not of good repute.

234. *Criterion 26.4* –

a) The Basel Committee Core Principles for Effective Banking Supervision and the IAIS Insurance Core Principles have been transposed into Lithuanian law by the resolution of BoL Management Board No.22 on the Effective Banking Supervision Principles and by the resolution of BoL Management Board No. 03-354 on the Main Principles on the Insurance Supervision). The Objectives and Principles for Securities Regulation issued by IOSCO Commissions have been transposed into The Markets in Financial Instruments (Art. 107 stating the main requirements for consolidated supervisions for investment firms). Banking, insurance and investment firms groups are required to implement group-wide policies and procedures (including but not limited to ML/FT) for sharing information. Banking, insurance and investment firm groups are regulated and supervised in line with the core principles. The BoL exercises consolidated group-wide AML/CFT supervision in practice.

b) The BoL sets risk-based supervision principles for all supervised entities (incl. but not limited to AML/CFT supervision) through a series of written policies and procedures. These include the BoL Financial Market Supervision Policy; Risk-Based System Concept of the BoL Supervisory Services; Main Principles of AML/CTF Risk-Based Supervision as a Part of Operational Risk Supervision; the AML inspection methodology and the Evaluation of the Risk Profile of the Insurance Companies. In addition, there are Rules of Providing Information to the Bank of Lithuania about Banks' Internal Control and Activity. The Main Principles of AML/CTF Risk-Based Supervision as a Part of Operational Risk Supervision defines supervisory actions (i.e. intensity/frequency of off-site and on-site supervision) for all risk categories as well as for each entity within a specific category. It also elaborates key differences in risk evaluation and supervision in the AML/CFT and prudential areas. Overall, these documents combine to produce a programme of supervision predicated on prudential rather than on AML/CFT supervision. Nevertheless, they allow for some strong elements of AML/CFT risk-based supervision to be undertaken in practice, including in relation to consolidated group supervision. Also see IO.5.

235. *Criterion 26.5* – See c.26.4. Off-site and onsite AML/CFT supervision is undertaken by the BoL and include strong elements of risk-based AML/CFT supervision. Offsite supervision includes reviews of annual AML/CFT questionnaires completed by all FIs (quantitative and qualitative non-structured data reporting) which is updated on an annual basis. In addition, quarterly prudential compliance, risk and internal audit reports from banks, major bank branches and central credit union are taken into account. Also see IO.3.

See c.24.4 and 24.6. According to the Risk-Based System Concept the BoL attributes FIs to four sectoral categories with the aim of distributing overall supervisory resources so as to pay more attention to the largest market participants whose activities are potentially (but not necessarily) subject to higher ML risks. Each institution in the first category of the institutions (banks) is awarded an overall operational risk rating; each bank is also formally rated for AML/CFT purposes but this is a factor in informing, and is part of, the BoL's overall operational risk categorisation which it uses to focus the frequency and intensity of its supervision. In addition, the AML/CFT division of the BoL uses the AML/CFT rating to inform its approach and, in practice, the AML/CFT division has been able to subject those FIs it considers should be subject to onsite inspections to such inspections. Other FIs receive a conceptual and informal AML/CFT risk rating, which also informs its approach. The approach to assessing risk and forming conclusions on the AML/CFT risk of FIs is not articulated in writing. Nevertheless, overall, in practice the frequency and intensity of AML/CFT supervision in relation to individual institutions and groups has strong elements of AML/CFT risk-based supervision. Information acquired during the licensing process includes the FI's internal policies and procedures) and is used as a primary indicator for determining the FI's risk profile in practice. In addition, information about internal control procedures is acquired from the annual offsite questionnaires as well as from quarterly reporting from banks, management reports, AML/CFT risk assessment reports, audit reports etc.). This information is considered as an input for risk rating banks and also for identifying the other riskier FIs.

Information from the NRA (and in practice the EU Supranational Risk Assessment) forms part of the AML/CFT risk factor used for determining the FI's overall risk level and frequency and intensity of on-site and off-site supervisory activities. The Principles of AML/CTF Risk-Based Supervision as a Part of the Operational Risk Supervision state that the risks identified during the NRA should be taken into account while performing AML/CFT risk analysis. As the ML/FT risks identified in the NRA represent an input for categorising institutions in one of the four risk categories, the NRA is also a factor in the intensity of overall supervision. ML/FT risks present in Lithuania are considered as part of the AML/CFT supervisory approach.

Although not articulated in a written document, the sectoral characteristics of FIs and groups, and particular the diversity and number of FIs, are also taken into account in its supervision for AML/CFT purposes.

236. *Criterion 26.6* **–** See c.26.5 for the approaches to risk profiling. The formal AML/CFT risk rating provided for the entities belonging to the first risk category under the Risk-Based System Concept (banks) is reviewed at least once per year but only as part of prudential risk supervision falling under the operational risk. The frequency of the reviews of the risk profile of the entities belonging to categories 2-4 is based on triggers or on the analytical selection. In addition, the risk categories – all four of them - are reviewed each year. The Risk-Based System Concept is reviewed every 3 years. In practice, the AML/CFT risk rating (the formal rating for banks and the conceptual informal rating for

other FIs) is considered each time there are major events or developments in the management and operations of an FI or group.

Weighting and Conclusion

237. The extensiveness of the requirements to prevent criminals from involvement with control of FIs is not clear. While AML/CFT is a factor in supervision and risk ratings by the BoL, AML/CFT supervision has strong elements of risk-based approach. **R.26 is rated PC.**

Recommendation 27 – Powers of supervisors

238. Lithuania was rated C with the previous R.29.

239. *Criterion 27.1* – Art. 3 and 4(1) of the AML/CFT Law authorise the BoL and the FIU to approve instructions aimed at preventing ML and FT, supervise the activities of supervised entities with regard to the implementation of ML/FT preventive measures and advise these entities on issues concerning the implementation of AML/CFT requirements.

240. *Criterion 27.2* – Art. 32 of the AML/CFT Law authorises supervisors to carry out inspections. In addition, other laws provide for inspections to be carried out by the BoL, for example: Law on Banks (Art. 42 and 69), Law on Financial Institutions (Art. 4(3)), and Law on Credit Unions (Art. 59).

241. *Criterion 27.3* – The BoL and the FIU have the right to obtain information and documents (Art. 32, paragraph 1 (4, 5 and 8) AML/CFT Law).

242. *Criterion 27.4* – Art. 33 of the AML/CFT Law authorises supervisory authorities to impose sanctions on supervised entities for breaching the AML/CFT requirements. Art. 36 (and Art. 198 of the Code on Administrative Offences) provides the following sanctions:

a. warning;
b. fine (see next par.);
c. temporary suspension from duties of the board member/members, the director/directors of administration or a senior manager of the FIs or other obliged entities and the director/directors of a branch of foreign FIs or other obliged entities, or suspension from duties of the board member/members, the director/directors of administration or a senior manager of the FIs or other obliged entities and the director/directors of a branch of foreign FIs or other obliged entities requiring that they be removed from office and/or a contract concluded therewith be terminated and/or they be divested of their powers;
d. temporary or permanent prohibition/restriction of activities of one or several branches or other establishments of the FIs or other obliged entities;
e. temporary restriction of the right of the FIs or other obliged entities to dispose of the funds on accounts held with credit institutions and/or of other property;
f. withdrawal of the licence or authorisation to pursue activities or temporary suspension thereof until the breach of this Law persists;
g. temporary prohibition for the FI to provide one or several financial services.

243. The BoL and the FIU have the right to impose the following fines on a FI or a branch of a foreign FI:

a) for breaches of the Law – from 0.5 up to 5 per cent of total annual income;

b) for breaches of the Law, where the FI or the branch of the foreign FI commits systematic breaches of the Law or commits a single serious breach of the Law or commits a repeated breach of this Law within a year from the imposition of a sanction for the breach of this Law – from 0.5 up to 10 per cent of total annual income (where 10 per cent of the total annual income exceeds EUR 5,100,000), or from EUR 2,000 up to EUR 5,100,000 (where 10 per cent of the total annual income does not exceed EUR 5,100,000);

c) for failure to provide, within the fixed time limit, information or documents required for supervisory purposes on the basis of this Law or for the provision of incorrect information – from 0.1 up to 0.5 per cent of the total annual income;

d) for failure to comply or inadequate compliance with the mandatory instructions issued by the supervisory authority pursuant to this Law – from 0.1 up to 1 per cent of the total annual income;

e) for improper performance of the actions which it has the right to perform only upon obtaining an authorisation from the BoL and the FIU or for the performance of the actions without obtaining an authorisation from these authorities, where such an authorisation is required – from 0.1 up to 1.5 per cent of total annual income;

f) the BoL and the FIU have the right to impose a fine ranging from EUR 2,000 up to EUR 5,100,000 on a participant of a FI for breaches of the Law committed by the FI where it commits systematic breaches of the Law or commits a single serious breach of the Law or commits a repeated breach of the Law within a year of the imposition of a sanction for the breach of the Law.

244. The BoL and the FIU have the right to impose more than one sanction (Art. 36(11)).

245. Licences/registrations may also be withdrawn under Art. 46 AML/CFT Law. In addition, there are provisions for the publication of sanctions in Art. 41.

Weighting and Conclusion

246. All criteria are met. **R.27 is rated C**.

Recommendation 28 – Regulation and supervision of DNFBPs

247. Lithuania was rated PC with the previous R.24. The 4th round MER concluded that certain activities or professions (such as company services providers) were strongly exposed to ML/FT risks given the absence of any sector-specific regulations and licensing/authorisation; there were some legal limitations for supervisory authorities and self-regulatory bodies to carry out their supervisory function, mainly concerning lawyers and assistant lawyers; the AML Law did not require licencing of internet casinos; and there were several effectiveness issues concerning the supervision.

248. *Criterion 28.1* –

a) Gambling companies are required to be licensed under Art .4 of the Gaming Law.

b) Under Art. 11 of the Gaming Law persons with a non-spent or valid conviction for serious or very serious deliberate crimes or crimes against property, property rights, property interests, the economy and business practice or the financial system may not be the founders (shareholders) of a gaming company or its controllers, members of its supervisory council and board of directors, heads of the administration and their deputies, chief financiers, heads of the administration of a gaming establishment (casino), bingo hall or gaming machine hall and their deputies, chief financiers, or staff members providing services to the players. A controller is defined as meaning a natural or legal person which (1) has the right to elect (appoint) more than half the members of the supervisory council (board of directors) or the head of the administration; or (2) exercises actual control over the decisions made by a legal person: has the right of ownership to all or part of the assets of an economic entity or the right of disposal in respect of all or part of such assets. This definition does not cover all potential beneficial owners in practice. In practice, the GCA has required information to be provided on all beneficial owners (with no threshold applied) for the four casinos with beneficial owners and no issues have arisen. Associates of criminal are also not covered.

Art. 4 and 11 of the Gaming Law and Arts.9, 12 to 15, 17, 20 and 25 provide powers for the GCA to deal with applications such as requiring information to be provided to it and to refuse an application.

Under Art. 12 of the Gaming Law changes to shareholders of licensed establishments should be notified to the GCA within 30 days of the change; under Art. 25 of the Licensing Rules changes to the officers specified above must be advised to the GCA within 5 business days. Controllers can be removed under Art. 11 of the law although this requires an application to be made to the court. The evaluation team does not consider the 5/30 day timeframe before notification to the GCA and the lack of ability of the supervisor to address problems by itself as fully meeting the criterion.

c) Under Art. 4 of the AML/CFT Law the FIU and the GCA have authority for supervising compliance by gaming entities; a MoU between the two authorities providing for clarity of functions. The sanctions framework specified in c.28.4 is applicable to the FIU and the GCA.

249. *Criteria 28.2 and 3* – Art. 4 of the AML/CFT Law designates supervisory authorities for other categories of DNFBP and as responsible for monitoring AML/CFT compliance. With regard to those specified by the FATF the position is as follows:

a) Lithuanian Bar Association: advocates;

b) Chamber of Notaries: notaries;

c) LAO: persons engaged in economic and commercial activities related to trading in precious metals and stones.

250. Art. 4(9) provides that the FIU shall approve instructions aimed at preventing ML/FT for the following DNFBPs:

a) undertakings providing accounting or tax advisory services;

b) providers of trust or company incorporation or administration services (TCSPs);

c) persons engaged in economic and commercial activities involving trade in precious stones, precious metals, movable cultural goods, antiques or any other property the value whereof is equal to or exceeds EUR 10,000 or an equivalent amount in foreign currency;

d) real estate agents/brokers.

251. The FIU also has a responsibility to supervise compliance by all DNFBPs with regard to ML/FT. The supervisory authorities (where the FIU is not the supervisor in practice) and the FIU must, in accordance with a mutually determined procedure, cooperate and exchange information about the results of AML/CFT inspections of reporting entities' activities. MoUs have been signed between the FIU and each of the supervisory authorities.

252. There is no registration framework in place for TCSPs (there appear to be no TSPs and most CSPs appear to be lawyers), accountants and real estate agents. There is not a complete system in place to monitor AML/CFT compliance by these entities although the FIU has undertaken onsite inspections to some of them. In addition, the assessment team has not been provided with information on the MoJ's framework for registering notaries.

253. *Criterion 28.4* –

a) Art. 32 of the AML/CFT Law provides the supervisory authorities with powers to perform their functions:

i. right to request information/explanations;

ii. right to request an obliged entity representative(s) to be interviewed at the supervisor's premises;

iii. right to interview any other representative or person who agrees to be interviewed in order to obtain information related to the subject of inspection;

iv. unimpeded access to the premises of the supervised obliged entities (except from the premises of advocates and their assistants), during their working hours, to inspect documents, notes of the employees, accounting documents and other data (including a bank secret or any other confidential information), to obtain copies and extracts of the documents, to copy the information stored in computers and any other electronic devise, and to seek advice/expert opinion from the specialised bodies or experts;

v. right to temporarily seize the documents of the supervised obliged entities (except those of advocates and advocates' assistants), that may evidence any breach of compliance. Seizure of the documents needs to be notified in writing, including the reasons for seizure and list of documents seized;

vi. right to seal a premise used by the obliged entities wherein documents subject to the examination and seizure are held for the period and to the extent necessary to carry out the inspection. This measure can be applied for no longer than three calendar days;

vii. right to use technical devices/support in the course of inspection;

viii. right to obtain information on subscribers or registered users of electronic communications services, (except from users who are advocates and their assistants), the traffic data and the content of information transmitted by electronic communications networks from providers of the electronic communications networks and/or public electronic communications services (this action can only be carried out with the judicial authorisation); and

ix. right to obtain data and documents or copies thereof related to the person(s) under inspection from other entities, including those from state and municipal institutions.

The Bar Association and the Chamber of Notaries have the right to exercise the powers stipulated in points i), ii), vii) and ix) above but not the other powers.

b) Art. 25 AML/CFT Law provides that a person may not be the beneficial owner of a real estate agency, or a member of the management or supervisory body of such entity, if he/she has been convicted of a crime against property, property rights, property interests, the economy, the order of business, the financial system, civil service and public interests, and if the conviction has not expired or has not been expunged. It is not clear that this would cover all relevant criminality. These provisions also apply in relation to TCSPs.

Art. 3 of the Law on the Notaries Profession provides that a person cannot be appointed as a notary if he/she has been convicted of a serious crime. Where a person has been convicted of any other crime (ie not a serious crime) he/she can be appointed as a notary, but only if 5 years have passed since the sentence, the suspension of the sentence or a release from a sentence). In addition, a notary must be of impeccable character.

The Law on the Bar (Art. 7) provides requirements for a person seeking to practice as an advocate, among which there is a requirement to be of high moral character. In addition, Art. 8 states that an applicant may not be recognised as an advocate if he/she (1) has been convicted of a serious or very serious crime until the conviction has expired or been lifted and at least four years after the execution or release of the sentence have passed (2) has been convicted of another intentional crime until the conviction has expired or been lifted and at least three years have passed since the sentence, the suspension of the sentence or the release of the sentence (3) has been found guilty of intentional crime, however released from the sentence (4) does not meet the requirements laid down for advocates in the Lithuanian Code of Ethics for Advocates.

The provisions for DNFBPs do not cover associates of criminals.

c) Art. 36 AML/CFT Law (and Art. 198 of the Code on Administrative Offences) specifies the administrative sanctions available in case of failure to comply with AML/CFT requirements (see c. 27.3).

DNFBP supervisory authorities but not including the Lithuanian Bar Association and the Chamber of Notaries have the right to impose the following fines:

i. for breaches of the Law – from 0.5 up to 5 per cent of the annual income from professional or other activities;

ii. for breaches of the Law, where an entity commits systematic breaches of the Law or commits a single serious breach of the Law or commits a repeated breach of the Law within a year of the imposition of a sanction for the breach of the Law – up to twice the amount of the benefit derived from the breach (where such benefit can be determined and where this amount exceeds EUR 1,100,000), or from EUR 2,000 to EUR 1,100,000 (where the amount which is twice the amount of the benefit derived from the breach does not exceed EUR 1,100,000 or the amount of the benefit derived from the breach cannot be determined);

iii. for failure to provide, within the fixed time limit, the information or documents required for supervisory purposes on the basis of the Law or for the provision of incorrect information – from 0.1 up to 0.5 percent of the annual income from professional or other activities indicated in Art. 2(10) of the Law;

iv. for failure to comply or inadequate compliance with the mandatory instructions issued by the supervisory authority pursuant to the Law – from 0.1 up to 1 percent of the annual income from professional or other activities indicated in Art. 2(10) of the Law;

v. for improper performance of the actions which an entity has the right to perform only upon obtaining an authorisation from the supervisory authority or for the performance of the actions without obtaining the authorisation from the supervisory authorities, where such an authorisation is required – from 0.1 up to 1.5 percent of the annual income from professional or other activities indicated in Art. 2(10) of the Law.

vi. where a DNFBP commits systematic breaches of the Law or commits a single serious breach of the Law or commits a repeated breach of the Law within a year from the imposition of a sanction for the breach – up to twice the amount of the benefit derived from the breach (where such benefit can be determined and where this amount exceeds EUR 1,100,000), or from EUR 2,000 up to EUR 1,100,000 (where the amount which is twice the amount of the benefit derived from the breach does not exceed EUR 1,100,000 or the amount of the benefit derived from the breach cannot be determined).

The inability of the supervisory authorities for legal professionals and auditors to impose fines for AML/CFT breaches is a gap.

Licences/registrations may also be withdrawn under Art.46 of the AML/CFT Law. In addition, there are provisions for the publication of sanctions in Art. 41.

254. *Criterion 28.5* –

a) See IO.3. None of the DNFBP supervisory authorities has a comprehensive approach to AML/CFT supervision (including a risk sensitive approach).

Casinos – the Risk Assessment and Management Methodology articulates the GCA's risk-based approach to supervision. There are four risk categories, with an equal number of entities in each category, and the GCA must annually evaluate the risks of all gaming establishments. The methodology specifies a range of risk factors; it is partially AML/CFT risk-based. Higher risk establishments are given priority with regard to inspections.

Dealers in precious metals and stones – The LAO has selection criteria providing that the identification of risks is based on a range of criteria, including information from previous inspections; Customs import/export data; and information from the FIU. These criteria are mostly not specifically aimed at AML/CFT but in addition to intelligence from the FIU and information from previous inspections, some other elements are partly relevant for AML/CFT purposes.

Notaries – Under the Law on the Notaries Profession (Art. 4), the assessment of notaries (which includes assessing compliance with relevant AML/CFT requirements) takes place a year after the notary has started providing professional services. Follow up assessments are undertaken every five years. More frequent and intensive supervision is carried out in cases the notary breaches the professional norms while providing services, or if there are other grounds to reasonably doubt the notary's competence (e.g. complaints on his/her professional performance).

Advocates – The supervision of advocates is carried out in accordance with the Law on Bar (Art. 52) and the Description of Procedure for Solving Disciplinary Cases of Lawyers (paragraph 7). Art. 52 of the Law deals with the hearing of disciplinary actions against Advocates. AML/CFT risk is not assessed and AML/CFT supervision is not undertaken.

Trust and Company Service Providers, Real Estate Agents, Accountants and Auditors - In the absence of a register the FIU forms views on which entities to inspect from when the sector in question was last subject to inspections, whether the sector is new, information in public sources,

such as the media, and its intelligence. The selection of firms is based on receipt of complaints, information about potential illegality or non-compliance with legislation, and ensuring that violations found at previous evaluations have been remedied. The sectors and firms selected arise from discussion at a meeting of staff of the FIU so that as much intelligence as possible on financial intelligence can be used for the selection process.

b) The approaches of the DNFBP supervisors take into account ML/FT profiles of individual DNFBPs to the extent mentioned above. With regard to written polices/procedures, the FIU's onsite checklist refers to controls and polices and the LAO's onsite questionnaire refers to procedures. Onsite inspections undertaken by the GCA and the FIU consider risk, controls, policies, and procedures and by extension the degree of discretion allowed by AML/CFT requirements while the LAO checks that procedures exist.

Weighting and Conclusion

255. A registration framework for TCSPs, accountants and real estate agents is not in place. While there are statutory powers to prevent criminal control of DNFBPs, the coverage of this is not clear except in relation to advocates. The Bar Association and the Chamber of Notaries do not have complete statutory powers in relation to supervision and sanctions. Associates of criminals are not covered. There are gaps in relation to risk sensitive supervision. **R.28 is rated PC.**

Recommendation 29 - Financial intelligence units

256. In the previous MER, Lithuania was rated PC with the requirements related to the FIU. Deficiencies pertained to the insufficient legal framework covering the actual FIU functions, its operational independence and the absence of fully fledged analysis of FT.

257. *Criterion 29.1* – The entity designated as an FIU under the AML/CFT Law is the FCIS (Art. 5). The FCIS, which is a LEA accountable to the Ministry of Interior (Art. 2, FCIS Law), formally designates its FIU functions to the Money Laundering Prevention Board (MLPB), which is the *de facto* FIU. The MLPB is an administrative unit of the FCIS established by an order of the Director of the FCIS: the *Regulations of the Money Laundering Prevention Board of the Financial Crime Investigation Service* (Order No V-258 of 18 November 2013 – hereafter "MLPB Regs"). The FIU powers and duties of the FCIS set out in the AML/CFT Law are mirrored in the MLPB Regs. Pursuant to the MLPB Regs, the MLPB is responsible for the implementation of ML and FT prevention measures and disclosing crimes, other criminal offences related to ML, FT and related crimes and other breaches of the law (Clause 4.2 and 4.3 MLPB Regs). The FIU performs the following functions: (1) the collection, registration and analysis of information from public authorities, FIs, and other legal and natural persons on customers and related financial operations and transactions; and (2) having identified possible indications of criminal offences or other breaches of the law, the referral of materials collected during its analysis for further investigation to other administrative units within the FCIS and other domestic or foreign authorities (Clause 5.1 and 5.3 MLPB Regs).

258. *Criterion 29.2* – (a) The MLPB receives reports on suspicious monetary operations and transactions related to ML/FT filed by reporting entities (Art. 16 AML/CFT Law). (b) The MLPB also receives reports on cash transactions exceeding EUR 15,000 (Art. 20 AML/CFT Law).

259. *Criterion 29.3* – The MLPB may request information from all reporting entities and domestic authorities to perform any of its functions and irrespective of whether an STR has been received (Art.

7(1) and (2) AML/CFT Law; Clause 6.1, MLPB Regs). It has direct online access to a wide range of database which contain financial, administrative and law enforcement information.

260. *Criterion 29.4* – The MLPB conducts operational analysis as described under core issue 6.3 of this MER. Some strategic analysis is also carried out, although not in a systematic fashion.

261. *Criterion 29.5* – The MLPB, after having identified indications of criminal offences or other breaches of the law, refers materials collected during its analysis for further investigation to other FCIS administrative units and other domestic or foreign authorities (Clause 5.3 MLPB Regs). The FIU exchanges information with all LEAs in Lithuania upon request. The decision on disseminating information to LEAs remains with the FIU. Materials and information are transmitted through secure channels by encrypted connections using e-signatures.

Criterion 29.6 –

(a) Clause 10.9 MLPB Regs state that the Head is responsible for ensuring the main principles of the organisation of the protection of classified information established by the Law on State Secrets and Official Secrets. By order of the Minister of Internal Affairs, the staff of the FIU is subject to the rules governing the security and confidentiality of information in Gov. Res. 966 (2016).

(b) Depending on the security clearance level (restricted, secret, top secret) special clearance cards are issued for FCIS employees. Permission to work with restricted, confidential, secret or top secret information is given by the SSD after the necessary checks are carried out. The premises are also divided to different security areas. Training is provided each year to all officers of the FCIS.

(c) Physical access to the MLPB premises is restricted by a passcode which is only available to employees. The FIU internal database is not accessible to other FCIS units (confidential order of the Director of the FCIS on Money Laundering Prevention information system). However, on the basis of special filters, officers of other units of the FCIS may check whether a person features in the database of the FIU. Where a hit is identified, they may request additional information from the FIU.

262. *Criterion 29.7* –

(a) In the 2012 MER, Lithuania was criticised for not having a clear legal framework for the structure and position of the entity performing FIU functions within the FCIS and the lack of legal safeguards to ensure its operational independence. To address these shortcomings, the MLPB was created as an autonomous division within the FCIS by virtue of the MLPB Regs. The responsibility for the activities of the MLPB is vested in the Head of the Board, who plans, organises and controls the work of the MLPB. The Head is appointed and dismissed by and directly subordinated and accountable to the FCIS Director. The MLPB may only be reorganised or liquidated by the Minister of Interior (Clauses 8, 9, 10 and 13 MLPB Regs). The FIU autonomously takes the decision to analyse, request and disseminate information. However, it is the Head of the FCIS which signs reports before they are disseminated to LEAs.

(b) The MLPB Head represents the Board and cooperates with foreign authorities and international organisations within the remit of the MLPB (Clause 10.7 MLPB Regs). The Head of the MLPB signs MoUs with foreign FIUs. The MLPB may obtain information from all domestic authorities and the FCIS (Clause 6.1 and 6.2 MLPB Regs). However, the Head of the FCIS is required to sign off all requests for information, as a matter of formality.

(c) While the MLPB is located within the FCIS, its functions are distinctly set out in the MLPB Regs.

(d) A working group is formed in the FCIS to prepare a draft strategic plan which includes the budget amounts intended for AML/CFT purposes. The MLPB Head takes part in the working group. With the assent of the FCIS Director, the draft strategic plan is submitted to the Minister of Interior for approval. The FCIS Director is accountable for budget expenditure.

263. *Criterion 29.8* – The FIU of Lithuania, under its various forms, has been a member of the Egmont Group since 1997.

Weighting and Conclusion

264. Lithuania is compliant with most of the criteria, except for C.29.7, which is mostly met and C.29.4 which is mostly met. While the FIU has functions which are distinct from those of the FCIS, as a matter of formality, it is the Head of the FCIS which signs off requests for information and reports disseminated to LEAs. Strategic analysis is not conducted in a systematic fashion. **R.29 is rated LC**.

Recommendation 30 – Responsibilities of law enforcement and investigative authorities

265. In the 2012 MER Lithuania was assessed as LC on the requirements of the former R.27. The deficiencies identified were related to effectiveness issues (e.g. low level of ML investigations).

266. *Criterion 30.1* – In Lithuania, all LEAs can investigate ML, associated predicate offences and FT. In practice, most ML and FT cases are investigated by the FCIS, which is an autonomous law enforcement body under the Ministry of Interior responsible for the investigation of violations of law against the financial system and related crimes (FCIS Law). The SIS conducts ML investigations related to corruption offences. The Police also conduct ML/FT pre-trial investigations. At the Police, ML pre-trial investigations are carried out by a specialised unit dealing with crimes against property (Order of General Commissioner of Police No. 5-V-890, 17 October 2014).

267. All pre-trial investigations, including those for ML and FT, are organised, conducted and supervised by the Prosecution Service (Art. 170 and 171 CPC). Since 2017, ML pre-trial investigations have been overseen by specialised units dealing with ML and unjust enrichment (Order No. I-68, 7 March 2017). Such units have been set up both at the PGO (within the Department of Criminal Prosecutions) and at the regional (though not in the district) offices.

268. Regarding FT investigations, in accordance with the PG's Recommendations on Specialisation, there is a separate specialisation for crimes against public security (which comprise FT as defined by Art. 250(4) CC) in the Department for Organised Crimes and Corruption Investigation of the PGO and in specialised Organised Crime and Corruption Investigation Divisions of regional prosecutor's offices. A prosecutor was appointed at the PGO to specialise in terrorism crimes. The Lithuanian Criminal Police Bureau has specialised divisions for the investigation of terrorism crimes and FT.

269. *Criterion 30.2* – A financial investigation must be carried out with respect to all crimes related to possible direct or indirect criminal material gain (Clause 3 of the PG Recommendations on Financial Investigations). Financial investigations may either be carried out before or during a pre-trial investigation of a predicate offence. Where the material gain does not exceed EUR 1,500, only a simple financial investigation is required. The purpose in these cases is to identify the property that could potentially be subject to confiscation. Otherwise, a fully-fledged financial investigation is compulsory.

270. *Criterion 30.3* – All LEAs are required to identify, trace and initiate freezing and seizing of property under the PG's Recommendations on Financial Investigations.

271. *Criterion 30.4* – There are no competent authorities in Lithuania, which are not LEAs but have responsibility for pursuing financial investigations of predicate offences.

272. *Criterion 30.5* – Lithuania designated the Special Investigation Service of Lithuania as a national competent authority that may assist other States Parties in developing and implementing specific measures for the prevention of corruption, in accordance with Art. 6(3) of the United Nations Convention against Corruption. The SIS has the same powers as all other LEAs in Lithuania.

Weighting and Conclusion

273. All criteria are met. **R.30 is rated C**.

Recommendation 31 - Powers of law enforcement and investigative authorities

274. In the 3rd Round MER of 2006, Lithuania was rated C with the former FATF R.28; hence this recommendation was not assessed in Lithuania's 4th Round MER of 2012. The new R.31 contains more detailed requirements.

275. *Criterion 31.1* –

(a) The process of obtaining the production of records held by FIs, DNFBPs and other natural or legal persons at the pre-trial investigation stage is regulated by Art. 155 CPC which provides that, upon issuing relevant decisions and obtaining the consent of the pre-trial judge, the prosecutor is entitled to arrive at the premises of any state or municipal institution, public or private establishment, company or organisation and be allowed to familiarise himself with the relevant documentation or any other required information, to make entries or make copies of documents and information or to obtain specified information in writing if this is required for the purposes of investigation of a criminal offence. On the basis of the prosecutor's assignment a pre-trial investigation officer may also familiarise himself with information in accordance with the same procedure.

(b) Where there are grounds to assume that there are in some premises or in any other place or in the possession of some person instruments of a crime, tangible objects and valuables that were obtained or acquired in a criminal way, or certain things or documents which might be relevant to the investigation of the criminal offence, a pre-trial investigation officer or a prosecutor may conduct a search for the purposes of discovering and seizing them (Art. 145 and 146 of the CPC).

(c) Witness statements are covered under Art. 178 CPC.

(d) When it is necessary to obtain important items or documents for the investigation of a criminal act and the location or possessor thereof is known, a pre-trial investigation officer or prosecutor may carry out seizure based on a grounded ruling issued by a pre-trial judge. Where persons possessing the items or documents fail to surrender them, seizure can be carried out with the use of force.

276. *Criterion 31.2* –

(a) LEAs may conduct covert operations during a pre-trial investigation. This includes carrying out (i) investigations without disclosing the identity of investigation offices, (ii) actions simulating a criminal act, and (iii) secret surveillance of a person, vehicle or object (Art. 158, 159 and 160 of the CPC). The measures must be authorised by a pre-trial judge upon the application of a prosecutor.

(b) During a pre-trial investigation, an officer may wiretap and keep records of conversations, transmitted through electronic communications networks, monitor and keep records of any other information transmitted through electronic communications networks and accumulate such information, if there are grounds to believe that the information may assist in identifying a crime in preparation, in progress or if the crime has already been committed (Art. 154 of the CPC).

(c) For the purposes of accessing computer systems, the device can be seized by way of carrying out search, seizure, recovery or voluntary provision (Art. 145, 147, 97 and 98 of the CPC) while the information retained in the computer system (other than the control of the flow of information being transmitted/received) is recorded by means of examination or inquiry into such a device (Art. 205-207 CPC). Inspections may be performed by pre-trial investigation officers alone or with the services of a specialist or be assigned to specialists. If a more detailed investigation or specific skills are needed to get into a computer system, IT expertise may be prescribed (Art. 208-210 CPC). More extensive recommendations thereof are provided in the PG's Recommendations on the Assignment of Tasks to Specialists and Experts. Meaningful information for an investigation, which was obtained during an inspection, an investigation of objects or an expertise may be copied to storage media and annexed to a case. If it is necessary to record a stream of information transmitted via electronic devices, Art. 154 CPC applies. If computer systems information that is meaningful for an investigation is located at companies, institutions or organisations, Art. 155 of the CPC applies.

(d) Controlled delivery is regulated by Art. 158 CPC, which is detailed in the PG's Recommendations for the Application of Criminal Intelligence and Criminal Procedure Code (par.52-54).

277. *Criterion 31.3* – Information on accounts may be obtained from the STI, which maintains an account register. It is not clear whether competent authorities can identify assets without prior notification to the owner.

278. *Criterion 31.4* – LEAs may obtain information from the FIU on the basis of the general powers to request information from domestic authorities set out in the laws under which they are constituted.

Weighting and Conclusion

279. It is not clear whether competent authorities can identify assets without prior notification to the owner. **R.31 is rated LC**.

Recommendation 32 – Cash Couriers

280. Lithuania was rated PC with the former FATF Special Recommendation IX during the 4th round MER in 2012. The main deficiencies affecting technical compliance pertained to gaps and inconsistencies in the cash-control regime.

281. *Criterion 32.1 and 32.2* – Lithuania has a declaration system in place. Any person entering Lithuania from a country outside the EU or leaving Lithuania to a country outside the EU is required to declare in writing cash in an amount which is equal to or exceeds EUR 10,000. Lithuania also has a disclosure system for intra-EU cash transportation. Disclosures shall also be made at the request of a customs officer in relation to sums exceeding EUR 10,000. (Art. 21 AML/CFT Law). Cash is defined in Art. 2(2) of Regulation (EC) No. 1889/2005 (Art. 2(8) AML/CFT Law) and includes bearer negotiable instruments. Since Art. 21 simply refers to persons entering or leaving Lithuania, the requirement applies at all borders – sea, air and land. The modalities of submitting written declarations are set out

in Order No 1B-1023 of 14 December 2016 issued by the Director General of the Customs Department. No requirements apply to mail and cargo.

282. *Criterion 32.3* – see c.32.1 for intra-EU cash transportation.

283. *Criterion 32.4* – Customs does not have the authority to request and obtain further information where a false declaration or disclosure, or failure to declare, has been detected.

284. *Criterion 32.5* – According to the practice of Lithuanian courts, persons who fail to declare cash exceeding EUR 10,000 when crossing the EU border with third countries are sanctioned under Art. 199(1) of the CC with the confiscation of all non-declared cash. Fines can be imposed according to the procedure of Art. 47 of the CC and their amount can be up to 300 MSLs (EUR 11,295). The assessment team considers these penalties to be proportionate and dissuasive.

285. According to Art. 5.2 of Order No 1B-1024 of 14 December 2016, at the request of customs the person shall submit the *Declaration on entering the Republic of Lithuania from third countries, or leaving it for third countries, or going through the Republic of Lithuania from a third country to a third country*, if the amount of cash carried is below EUR 10,000. In case of a false declaration or failure to submit a declaration under Art. 5.2, Art. 212 (Violation of the procedure for the declaration of goods (items)) of the Code of the Administrative offences will be applied.

286. *Criterion 32.6* – The Customs Department is required to notify the FCIS (MLPB) of a written declaration/disclosure within seven working days from receipt of the declaration.

287. *Criterion 32.7* – No information was provided co-ordination mechanisms among customs, immigration and other related authorities.

288. *Criterion 32.8* – There is no power to stop or restrain currency for a reasonable period of time in order to ascertain whether evidence of ML/FT may be found where there is a suspicion of ML/FT or predicate offences or when there is a false/non-declaration/disclosure.

289. *Criterion 32.9* – There are adequate mechanisms in place to ensure that Lithuania provides international cooperation and assistance in relation to the declaration system (Art. 6 and 7 of Regulation (EC) No. 1889/2005; Council Regulation (EC) No. 515/97 on mutual administrative assistance in customs matters). Outside of the EU, international cooperation takes place on the basis of a number of bilateral instruments and international conventions (Naples II, Nairobi Convention). In the course of pre-trial investigations or criminal proceedings, MLA may be sought and provided.

290. *Criterion 32.10* – There are safeguards in place to ensure the confidential handling of information collected through the declaration system. There is nothing to suggest that these safeguards would restrict trade payments or the freedom of movement of capital.

291. *Criterion 32.11* – The ML penalties would apply. See c.3.9 and 4.1.

Weighting and Conclusion

292. There are no requirements which apply to transportation of cash through mail and cargo. Customs does not have the authority to request and obtain further information where a false declaration or disclosure, or failure to declare, has been detected. There is no power to stop or restrain currency for a reasonable period of time in order to ascertain whether evidence of ML/FT may be found where there is a suspicion of ML/FT or predicate offences or when there is a false/non-

declaration/disclosure. No information was provided on cooperation at a domestic level. **R.32 is rated PC**.

Recommendation 33 – Statistics

293. In the 2012 MER, Lithuania was rated LC with former R.32. It was noted that: no reliable and consolidated statistics were kept on confiscation; the FIU's statistics were considered insufficient; the information system of the Prosecutor's Office needed improvements to usefully complement the police statistics; and there was no detailed statistics on cross-border movements of cash.

294. *Criterion 33.1* –

(a) Art. 28(6) AML/CFT Law requires the FCIS to keep the following data: number of reports on suspicious monetary operations or transactions; further measures taken concerning those reports; number of registered criminal acts of legalisation of property which derived from a criminal activity or provision of funding or support for terrorist activities and suspects, accused and convicts; data on predicate offences, where available; and number of STRs having led to ML/FT investigations and prosecution.

(b) Authorities advised that the Integrated Criminal Procedure System (IBPS), operational since February 2016, keeps data on pre-trial investigation for prosecution service and courts. This system has its own search mechanism, which enables generating statistical data by various criteria, including ML/FT-related data. The Information System of the Prosecution Service (IPS), operational since 2006, keeps data on pre-trial investigations. IPS is also connected with the integrated system of the courts (LITEKO) which is used to keep data about the court decisions.

(c) As per Art. 28 AML/CFT Law, the FCIS should also keep data on property which was subject to temporary restriction of the ownership rights, its value, property confiscated by a court decision and its value. The IBPS also keeps data on seizure and freezing orders.

(d) Art. 28 requires the FCIS to keep data on the number of FIU-to-FIU requests received, sent, replied to and rejected, as well as on MLA requests (incoming and outgoing) which concerned AML/CFT. The IPS keeps data on MLA requests received and sent including any other international communication instruments (European Arrest Warrant (EAW), European Investigation Order). The Document Management System has been in service since 2015 and keeps record of all official communication the prosecution service has with its counterparts (in-country and internationally). The MoJ also registers and keeps record of MLA requests – incoming and outgoing, including extradition. However, the statistics kept by the MoJ and the PGO are not categorised by legal qualification of a criminal act.

Weighting and Conclusion

295. The information data mechanism in place do not allow for the categorisation of MLA requests per legal qualification. **R.33 is rated LC**.

Recommendation 34 – Guidance and feedback

296. In the 2012 MER Lithuania was rated LC with the former R.25. Whilst the MER praised the country for having various guidance and instructions available to the different sectors, a lack of a

body which would ensure their consistency was noted. In addition, no guidance was issued to the legal professions.

297. *Criterion 34.1* – On feedback: Art. 5(1)(9) AML/CFT Law imposes an obligation to the FIU to notify FIs and/or other obliged entities, law enforcement and other state institutions, about i) the results of the analysis of the suspicious monetary operations or transactions report, ii) indications of possible ML and/or FT; and iii) breaches of the AML/CFT Law. See IO.6 - the key findings indicate that the FIU should hold awareness raising activities with reporting entities faced with a higher risk of ML/FT and provide more systematic feedback to reporting entities.

298. On guidelines: Art. 4(9) states that the FIU should provide methodological assistance to obliged entities. This concept includes the issue of guidance, trends, typologies and training. There is no similar provision for supervisory authorities responsible for AML/CFT supervision. The FIU participates in training events organised by the BoL and provides information on trends and typologies. It also works closely with DNFBP supervisors in providing information on suspicion, trends and typologies. See IO.3.

299. The BoL has been active in providing guidance although there is scope to do more. The Money Laundering and/or Terrorist Financing Prevention Guidelines for Financial Market Participants were issued in 2015. There is routine dialogue with FIs. In addition, the BoL routinely holds interactive compliance meetings which can be characterised as "question and answer" events. The results of thematic work are disseminated to FIs (Panama Papers, risk in the payment sector and cash). In 2016 and 2017 there were five training/briefing events. Overall, the topics covered are wide ranging, cover a wide range of market participants and there has been a focus on giving guidance of the revisions to the AML/CFT Law and on identifying and mitigating risk. DNFBP supervisory authorities have provided guidance but, overall, this has been relatively limited. In general, supervisory authorities work closely with the FIU so that guidance on detecting and reporting suspicion and trends and typologies is provided to reporting entities.

Weighting and Conclusion

300. Feedback by the FIU is not comprehensive. While there are no requirements/procedures for supervisory authorities to provide guidance, guidance is provided in practice, particularly but not limited to banks. Information on suspicion is provided. **R.34 is rated LC.**

Recommendation 35 – Sanctions

301. In the 2012 MER, Lithuania was rated PC with the former R.17. The assessors noted that the FCIS was not empowered to impose sanctions, fines and disciplinary actions (for both FIs and DNFBPs); the range of sanctions which could be imposed was not broad enough; and the maximum amount of sanctions which could be applied was not proportionate, effective and dissuasive for infringements committed by the larger economic entities.

302. *Criterion 35.1* –

303. The powers of sanction available to supervisory authorities are specified in C.27.4 and C.28.4. Art. 36 of the AML/CFT Law foresees a broad range of sanctions that might be imposed for reporting entities for breaches of the requirements stipulated under the law. The supervisory authorities for advocates and notaries do not have the power to impose fines for AML/CFT breaches.

304. Art. 34 (1) of the law considers the following to be a serious breach of the Law: 1) failure to comply with CDD requirements; 2) failure to comply with the requirements for reporting of suspicion; 3) failure to comply with the requirements for storage of information; 4) failure to comply with the requirements to set up internal control procedures as specified in the Law. Art. 34 (2) of the AML/CFT Law considers the following to be a systematic breach of the Law: 1) where a breach of the Law has been committed three or more times within a year from the imposition of a sanction for the breach of AML/CFT requirements; 2)where breaches of the law cover several groups of requirements.

305. Failure to comply with the requirements for reporting of suspicion is a serious breach for the purposes of the AML/CFT Law. However, notwithstanding the high administrative penalties which can be imposed, the assessment team is of the view that a criminal penalty should be applicable for the sanctioning framework for reporting of suspicion to be fully dissuasive. A tipping off provision is included in the AML/CFT Law (see C.21.2).While breach of the provision is covered by the sanctions in the law, it is not specified as a serious breach and is not subject to criminal liability.

306. All NPO regulators have access to a range of sanctions for failing to comply with relevant requirements. See analysis at C. 8.4(b).

307. With regard to TFS, Art. 123 Criminal Code provides that a person who violates international sanctions is potentially subject to a fine (no maximum is specified) or imprisonment of up to five years. The provision specifies that there is corporate liability.

308. *Criterion 35.2* –

309. Under Art. 39(2) of AML/CFT Law, the BoL and the FIU may impose a fine ranging from EUR 2,000 up to EUR 5,100,000 on senior managers and directors of FIs for breaches of the Law committed by the FI where it commits systematic breaches of the law, or commits a single serious breach of the law or commits a repeated breach of the law within a year from the imposition of a sanction for the breach of the law.

310. In addition, Art. 198 Code of Administrative Offences set the following sanctions for senior managers/directors:

- EUR 2,100 to 6,000 for violation of CDD and BO requirements;
- EUR 2,700 to 6,000 for violation of STR obligations and for non-implementing the measures aimed at protecting the information provided to the FIU; and
- EUR 2,000 to 3,500 for the violation of the procedure of implementation AML/CFT measures.

311. More dissuasive sanctions are foreseen in cases where managers/directors committed a violation repeatedly – EUR 3,500 to 5,800.

312. Overall, while significant fines are available to the BoL and the FIU, the framework for financial penalties for individuals is not fully dissuasive (noting also that advocates and notaries are not covered – see C.35.1).

313. Art. 36 of the AML/CFT Law also provides for senior managers and directors to be suspended, removed from office, their contract terminated and/or their powers removed. In addition, Art. 41 includes provisions on the publication of sanctions.

314. The provisions in relation to reporting of suspicion and tipping off in C.35.1 are also applicable for this criterion.

315. See C.35.1 for sanctions in relation to TFS.

Weighting and Conclusion

316. The supervisory authorities for advocates and notaries do not have power to impose fines for AML/CFT breaches. In addition, while there are fines, including significant fines, available for breaches by senior managers/directors, the maximum levels in all cases are not fully dissuasive. While sanctions are applicable, in the absence of criminal penalties the sanctions framework for reporting suspicion and tipping off is not fully dissuasive. **R.35 is rated LC.**

Recommendation 36 – International instruments

317. Lithuania was rated PC with both previous R.35 and SR.I in the 4th round, due to gaps in the ML and FT offence.

318. *Criterion 36.1* – As indicated in the 3rd and 4th round MERs of Lithuania, the country signed and ratified the Vienna, Palermo and Terrorist Financing Convention. The Merida Convention was ratified on 5 December 2006 and entered into force on 20 January 2007.

319. *Criterion 36.2* – Lithuania has provided information demonstrating that all relevant articles referred to in this criterion were fully implemented.

Weighting and Conclusion

320. All criteria are met. **R.36 is rated C**.

Recommendation 37 - Mutual legal assistance

321. In the 4th round, Lithuania was rated C with former R.36 and SR.V. It was not reassessed on former R.37, which had been rated C in the 3rd round.

322. *Criterion 37.1* – The Lithuanian competent authorities have a legal basis in place to provide the widest range of assistance in relation to investigations, prosecutions and related proceedings involving FT, ML, and associated predicate offences. Although, there does not seem to be an explicit obligation to provide cooperation "rapidly", in practice the authorities confirmed that this does not hinder their ability to provide assistance in a prompt manner.

323. With regard to judicial cooperation in criminal matters with other EU Member States, Lithuania applies the EU legal instruments through its Law on Mutual Recognition and Execution of the Decisions of the EU Member States in Criminal Proceedings (Law No XII-1322).

324. The CPC further contains provisions (Art. 365^3 and 365^4) on cooperation with EU member states for confiscation, implementing EU Framework Decisions 2005/212/JHA and 2006/783/JHA.

325. On 15 June 2017, Lithuania implemented the EU Directive on the European Investigation Order (EIO) through Law No XIII-397 amending Law No XII-1322. The Directive aims to reinforce the principle of mutual recognition of judicial decisions in the EU for the purpose of obtaining evidence for use in criminal proceedings.

326. *Criterion 37.2* – According to Art. 66(2) and 67(2) of the CPC, the courts and prosecution authorities shall transmit their requests to foreign authorities and receive the requests of foreign

authorities through the Ministry of Justice or the PGO (the central authorities). If a MLA request is received directly from foreign authorities, it may only be executed subject to authorisation by the central authorities (Art. 67(2) of the CPC). This condition does not apply to cases of direct communication provided for by international treaties to which Lithuania is a party (Art. 67(2) of the CPC).

327. Law No XII-1322 gives time limits for the decision to recognise or not an EIO received from another EU member state, in line with the EIO Directive. The decision shall be taken without delay but not later than within 30 days from its receipt or within the shorter time indicated in the specific Order. If the Order relates to the secure evidence from destruction or other conveyance, the decision shall be taken within 24 hours from its receipt if possible.

328. With regards to confiscation orders issued by courts of other EU member states, the Lithuanian courts must decide on recognition or refusal within 7 days (Art. 365^4 of the CPC).

329. Outside of the context of the EU, the domestic law does not provide any particular terms for the consideration or execution of requests for MLA. Lithuania has advised that the time needed to deal with MLA requests varies depending on the nature of the request, the type of assistance and the complexity of the case. According to the Explanatory Note issued by the Prosecutor General's Office in October 2014, in the pre-trial stage it is recommended to execute MLA requests within four months (if it is not possible the executing authority must provide an explanation). At the trial stage, the period between the receipt of the request and transmission of the response is one to three months but may be shorter in very urgent cases or in the absence of practical execution problems.

330. There are case management systems in place to monitor progress on requests.

331. *Criterion 37.3* – The Lithuanian authorities shall not refuse to provide assistance subject to the condition that these proceedings are not contrary to the Constitution, the laws and the fundamental principles of the criminal procedure of Lithuania. Lithuanian legislation does not establish any other list of special conditions for providing MLA. Optional grounds for refusal laid down in international treaties can be followed.

332. MLA is provided pursuant to the CPC, unless determined otherwise by international agreements provided that this is not contrary to the Constitution, the laws and the fundamental principles of the criminal procedure of Lithuania (Art. 67 of the CPC). Examples of fundamental breaches are the breaches of the requirements set forth in this Code resulting in the restriction of the accused rights assured by the law or prevented the court to examine the case in comprehensive and impartial manner and adopt a fair judgement or ruling. Decision on the possible breaches is a made on a case-by-case basis by the prosecutor or the court dealing with the incoming MLA.

333. Within the EU, all legal instruments related to international judicial cooperation are based on the principle of mutual recognition between Member States. However, the EIO Directive (Art. 11) outlines optional grounds for refusing to recognise or execute an EIO. Art. 365^3 CPC implements the grounds for refusing to recognize a confiscation order under the EU framework as mandatory grounds, which include situations where the enforcement of confiscation shall infringe fundamental human rights and/or freedoms or violate the prohibition to sentence a person for the same criminal offence for the second time. These conditions are not unreasonable or unduly restrictive.

334. *Criterion 37.4* – (a) Lithuania has ratified the Additional Protocol to the European Convention on Mutual Assistance in Criminal Matters of 1978 (entry into force in Lithuania in 1995) which

withdraws the possibility offered by the Convention to refuse assistance solely on the ground that the request concerns an offence which the requested party considers a fiscal offence.

(b) The CPC does not foresee that requests for MLA can be refused on the grounds of secrecy or confidentiality requirements on FIs and DNFBPs.

335. *Criterion 37.5* – The data of the criminal proceedings related to a foreign MLA request is subject to the same legal confidentiality regime as data on domestic proceedings under the CPC.

336. *Criterion 37.6* – In general, the dual criminality principle is not a ground for refusing MLA requests. However, some minor technical issues exist (see C.37.7).

337. *Criterion 37.7* – Authorities advised that if the offence by factual circumstances constitutes a criminal offence under the criminal laws of Lithuania, MLA shall be delivered regardless of the denomination of the offense in the requesting country. There is nothing in the legislation requiring that the offence described in a foreign country use the same terminology or fall within the same category of offence. The minor gaps in the Lithuanian FT and ML offences (see C.3.1, C.5.1) may limit the assistance that the country can offer to some extent.

338. *Criterion 37.8* – Art. 67(1) of the CPC stipulates that the competent authorities shall undertake proceedings set out in the CPC when carrying out requests of foreign authorities. Thus, domestic powers granted by the CPC can also be used in response to an MLA request. Deficiencies in domestic powers under the CPC (see R.31) would apply here. However, Art. 67(1) of the CPC also stipulates that, if provided for by international agreements, other actions that are not in the CPC may also be carried out if they do not contravene the Constitution, the laws and the fundamental principles of the criminal procedure of Lithuania.

Weighting and Conclusion

339. Lithuania has met or mostly met all criteria. There are however minor issues, including the absence of a legal provision to provide assistance rapidly and some minor gaps under C.3.1 and C.5.1 impacting criteria 37.6 and 7. **R.37 is rated LC.**

Recommendation 38 – Mutual legal assistance: freezing and confiscation

340. Lithuania was rated LC on R.38 in the 3rd round, since there were no arrangements to coordinate confiscation with other countries. Lithuania was not reassessed on R.38 in the 4th round.

341. *Criterion 38.1* – MLA for freezing and confiscation is conducted in accordance with the provisions of the CPC and ratified international agreements. The legal framework described under R.37 also applies to MLA in the field of freezing and confiscation. The cooperation with competent authorities of the EU Member States is regulated in Art. 365^3 and 365^4 of the CPC implementing EU Framework Decisions 2005/212/JHA and 2006/783/JHA. Art. 365^3 also provides for mandatory grounds for refusal of confiscation.

342. Overall, Lithuania has the authority to take appropriate action in response to requests by foreign countries to identify, arrest and confiscate proceeds from, instrumentalities used in or intended for use in ML, predicate offences or FT, and property of corresponding value. Confiscation is covered under Art. 72 of the CC, (see 2012 MER par.162-165). Also, Art. 1601 of the CPC provides for the use of procedural constraint measures in relation to search and seizure in urgent cases.

343. Outside of the EU framework, minor gaps in the FT criminalisation (see C.5.1) narrow Lithuania's powers to search and seize upon foreign request assets used in FT activity. See also relevant findings in relation to the Lithuanian framework to implement EU confiscation orders under R.37.

344. Minor gaps in the ML offence narrow possibilities to provide search and seizure of laundered property upon request by a non-EU state.[83]

345. *Criterion 38.2* – Foreign requests for assistance are executed in accordance with the CPC. The CPC foresees mandatory confiscation when criminal proceedings are terminated in absence of a conviction due to death of the perpetrator, where the perpetrator is unknown or unavailable by reason of flight or absence (Art. 94(1)(1) in combination with Art. 3(1) of the CPC).

346. *Criterion 38.3* – (a) Lithuania has arrangements for co-ordinating seizure and confiscation requirements. This could take the form, for instance, of joint investigations teams. There is extensive practice in this area. (b) Lithuania has mechanisms in place to manage and, where necessary, dispose of property frozen, seized, or confiscated, which also apply in relation to international requests (see C.4.4).

347. *Criterion 38.4* – The Resolution No. 219 of 13 March 2013[84] indicates how monetary property confiscated by Lithuania upon the order of another EU member state, shall be shared between the two countries. It does not regulate the sharing of other types of property. No information was provided on asset-sharing with non-EU countries or on asset-sharing when confiscation is indirectly a result of co-ordinated law enforcement actions.

Weighting and Conclusion

348. The Resolution No.219 does not regulate the sharing of other types of property. No information was provided on asset-sharing with non-EU countries or on asset-sharing when confiscation is indirectly a result of co-ordinated law enforcement actions. **R.38 is rated LC.**

Recommendation 39 – Extradition

349. Lithuania was rated C with former R.39 in the 3rd round and was not reassessed against these requirements in the 4th round.

350. *Criterion 39.1* – Art. 71-76 of the CPC regulate the surrender of persons under the EU Framework Decision 2002/584/JHA on the EAW and in instances provided for by international treaties in force in Lithuania. Lithuania has ratified the Council of Europe Convention on Extradition and its first, second and third additional protocols (but not its fourth).

(a) Both ML and FT are extraditable offences – they are punishable by imprisonment for more than one year, which is a necessary condition to consider a request for extradition under the CoE Convention on Extradition. The gaps in the FT and ML offences (see C.3.1, C.5.1) may limit the possibilities for extradition from Lithuania to some extent.

---

[83] The list of Article6 of the EU FD on confiscation, outlining categories of offenses to which the dual criminality principle does not apply, covers ML but not FT.

[84] Gov. Res. No. 219 "On the approval of the Rules of Transmission of Confiscation Orders Issued by Courts of the Republic of Lithuania for Execution to Other Member States of the European Union and procedure of allocation of monetary funds and assets obtained by execution of confiscation orders", 13 March 2013, amended by Gov. Res. No. 901, 3 September 2014.

(b) Art. 73 of the CPC sets out the procedure to be followed upon receiving a foreign request for extradition or an EAW. When the PGO receives an extradition request, it is translated into Lithuanian and brought before the Regional Court of Vilnius by the PGO. The Court must hold a hearing within seven days, upon which it shall issue an extradition order refuse the extradition. There are no deadlines for the court to issue an order. In case of insufficient information, the requesting authority shall be solicited immediately for more information. Appeal against an order is possible, and is to be lodged within seven days after the decision and to be heard within 14 days from its submission (Art. 74 of the CPC). There is no deadline for the court to issue an order upon the appeal after the hearing.

Art. 73(6) of the CPC lists considerations for the Court for prioritisation in case of several requests for the extradition of one person. Requests from the ICC prevail over other requests and requests for criminal prosecution prevail over requests to execute a penalty imposed by a judgment. In remaining cases, the Court must take in to account all circumstances for the extradition/surrender and consultations of international criminal prosecution institutions (including Eurojust).

Management systems are in place to monitor progress on the execution of requests. Once the decision on an EAW is effective, the surrender to the issuing country shall take place within ten days, or in exceptional circumstances, another date shall be set (Art. 76(2) of the CPC). For other extradition requests, the procedure and conditions of surrender are established by the international agreements and other legal acts (Art. 76(1) of the CPC).

(c) Art. 9(3) and Art. 71(3) of the CPC (containing identical provisions) list conditions under which 'it shall be allowed not to extradite' a person, which is understood to mean 'it shall not be allowed to extradite' (forming mandatory grounds for refusal).

Art. 9^1 of the CC contains a list of mandatory grounds for refusal (par.3 – e.g. amnesty; under-aged; statute of limitations) and a list of optional grounds (par.4), which apply to surrender of persons under the EAW. In principle, Lithuania retains exclusive competence for criminal acts committed on its territory, although ML and FT are both extraditable offenses. For extradition based on treaties, the fact that the crime for which extradition is sought was committed in Lithuania is a mandatory ground for refusal. It is an optional ground under the EAW. A mandatory ground for refusal under Art. 9(3) and Art. 71(3) of the CPC is when the person is being prosecuted for a crime of political nature.

351. *Criterion 39.2* –

(a) Lithuania has made a declaration under the European Convention on Extradition that it does not extradite its nationals. According to the declaration, this is based on Art. 6 of the Law on Lithuanian nationality (Citizenship Law). Art. 9 of the CC and Art. 13 of the Constitution prohibit the extradition of Lithuanian citizens, unless an international treaty establishes otherwise.

(b) Art. 68 of the CPC regulates actions to be taken by the PGO based on a request for prosecution by a foreign authority to initiate or to take over prosecution against a Lithuanian national who committed a criminal act in a foreign state and returned to Lithuania.

The conditions and procedure set in the CPC and in international agreements provide that upon receiving a request, the PGO shall determine whether this is based on reasonable grounds. These provisions do not contain any specific timeframe for the examination. However, in practice this is done without undue delay and there is no need to create a formal obligation to that effect. Art. 2 of the CPC gives a general duty to the prosecutor and institutions of pre-trial investigation to take all legitimate measures within their competence when elements of a criminal act are detected to carry out the investigation and reveal the criminal act 'within the shortest period of time'.

352. *Criterion 39.3* – Lithuanian law requires the presence of dual criminality to extradite or surrender a person based on a treaty (Art. 9(3)(1) of the CC; Art. 71(3)(1) of the CPC). Pursuant to Art. 9^1(3) of the CC, dual criminality shall not be verified if an EAW is issued for a criminal offence punishable under the law of the issuing member state by deprivation of liberty for a maximum period of at least three years, and if such a criminal offence is classified under the law of the issuing state as one of the offence categories listed in Art. 2(2) of the EU FD, which include ML but not FT.

353. Lithuania has advised that if, 'by factual circumstances', the criminal act for which extradition is sought constitutes a criminal offence under its criminal laws, extradition shall be provided in accordance with the CPC and ratified international instruments, regardless of the denomination of the offense in the requesting country. The 2006 MER (par.608) also found that the Court in Lithuania, when ruling to extradite a person, does not consider the technical differences between the laws of the requesting and requested countries such as categorisation or denomination of the offense. Only the description of acts and omissions has an importance for the court in determining whether the offense qualifies as 'crime'.

354. *Criterion 39.4* – Summary proceedings of extradition may be applied in cases provided for in international agreements or in case of an EAW (Art. 75 of the CPC). In 2017 Lithuania ratified the Third Additional Protocol to the European Convention on Extradition that foresees such a possibility. The Protocol seeks to simplify and accelerate the extradition procedure when the person sought consents to extradition. Under the simplified procedure of Art. 75 of the CPC, the Court must hold a hearing within three days and there is no possibility for its ruling is final. This procedure is only possible upon consent of the person subject to the extradition request/EAW and the approval of the PGO, which is to be confirmed by the Court at the hearing.

Weighting and Conclusion

355. Lithuania meets or mostly meets all of the four criteria under R.39. Some minor weaknesses relating to ML/FT offences may impact on the scope of application of extradition. There are no clear processes for timely execution of extradition requests. **R.39 is rated LC**.

Recommendation 40 – Other forms of international cooperation

356. In 2012 MER, Lithuania was rated LC with the requirements of R.40 on effectiveness grounds.

357. *Criterion 40.1* – The Lithuanian competent authorities have a legal basis in place to provide the widest range of information to their foreign counterparts in relation to ML, associated predicate offences and FT. Although, there does not seem to be an explicit obligation to provide cooperation "rapidly", in practice the authorities confirmed that this does not hinder their ability to exchange information in a prompt manner. Assistance can be provided both spontaneously and on request. The BoL, the Department of Cultural Heritage Protection, the GCA, the Lithuanian Bar Association, the Lithuanian Chamber of Notaries, the Lithuanian Chamber of Auditors, the Chamber of Judicial Officers of Lithuania and the LAO cooperate and exchange information with foreign institutions implementing ML and/or FT prevention measures (According to Art. 8 of the AML/CFT Law).

358. Art. 5 (par.6) of the AML/CFT Law provides for the FCIS to exchange information on possible criminal act or established indications of breaches of legal acts, collected during the analysis of the information received on the basis of this Law, with foreign institutions. The FCIS, as a member of the Egmont Group since 1999, exchanges information through the Egmont Secure Web encrypted

channel. Lithuania participates also in the FIU.Net initiative concerning exchange of information between EU Member States. In addition to these channels the Lithuanian FIU as a police-type unit is also involved in the Europol AWF work. In practice the information exchange pursuant to Order No. V-21 of the Director of the Financial Crime Investigation Service under the Ministry of the Interior of 31 January 2011 is carried out by the MLPD within the FCIS. The Lithuanian FIU may exchange information pursuant to the provisions of the AML/CFT Law and without the need of a memorandum of understanding.

359. Art. 19 of the Law on Criminal Intelligence provides for the exchange of criminal intelligence with partners, foreign LEAs, international organisations and EU agencies.

360. Art. 12 of the Police Law of the Republic of Lithuania provides the right and duty of the police to pursue international police cooperation. The Criminal Police Bureau also noted that its membership in different international bodies (Interpol, Europol, SIENA, Schengen area, CARIN Group, etc.) facilitates such cooperation. Relevant channels, including Eurojust, the EJN, the OLAF Anti-Fraud Communicators' Network (OAFCN), are used by the PGO in order to accelerate and improve the process of finding and recovering assets and providing other type of informal assistance.

361. Liaison Officers are also used for informal cooperation by the PGO. Contacts is being maintained via e-mails to Liaison Officers of Finland and Germany, residing in Lithuania and Lithuanian Liaison Officers residing abroad in order to address various questions related to criminal cases under investigation or receive feedback in the period prior or during an MLA request.

362. Art. 18 of the Law on Intelligence stipulates that the SSD has the right to exchange intelligence information with international organisations and institutions and competent authorities of foreign states.

363. Art. 28 to 30 of the Law on Tax Administration stipulate that the STI can exchange information with EU and other foreign state institutions. In relation to tax administration issues the STI can exchange information with its foreign counterparts under the Convention on Mutual Administrative Assistance in Tax Matters, Double Taxation Avoidance Treaties and EU directives and regulations both spontaneously and upon request. If available, the STI may provide the requesting competent tax authority with facts relating to ML when preparing a reply on tax issues. As regards the exchange of spontaneous information, it is submitted for taxation purposes, but if facts on ML are available, they are also included.

364. *Criterion* 40.2 –

(a) Generally, Lithuanian competent authorities have a legal basis for providing international cooperation: Art. 5 (par.6) of the AML/CFT Law for the FIU, Art. 18 of the Law on Intelligence for the SSD, Art. 68^1 of the CPC for the PGO, Art. 8 (par.2) of the AML/CFT Law for supervisors, the CPC for LEAs. Lithuania is also part of a number of international and bilateral treaties that provide a legal basis for international cooperation.

(b) All competent authorities have a legal basis for providing co-operation (AML/CFT Law: Art. 8(2) on supervisors, Art. 5(6) on the FIU; supplemented by relevant provisions in sectorial laws). There is nothing which hinders the competent authorities from using the most efficient means of co-operation. The following clear and secure gateways are used for the exchange of information: the Egmont Secure Web (FIU); Interpol and Europol (the NP); the European Judicial Network (EJN); the Schengen Information System (SIS)/SIRENE and European Arrest Warrant (EAW).

In addition, the PGO participates in the activities of various networks and expert groups meetings such as the Network of Prosecutors on Environmental Crime in the Baltic Sea Region (ENPRO); the European Judicial Cooperation Network for Criminal Matters (Eurojust), the national correspondent for terrorism matters, the Network of JITs, the Genocide Network, the Asset Recovery Network (CARIN), the European Judicial Training Network (EJTN), the Consultative Council of European Prosecutors (CCPE), the NADAL Network, the EU Consultative Forum of Prosecutors General and Directors of Public Prosecutions, and the Evidence Expert Group Meetings.

(c) The FIU (through the Egmont Secure Web and FIU.NET) and the LEAs (through INTERPOL and EUROPOL) use clear and secure channels, circuits and mechanisms to facilitate transmission and execution of requests. In urgent cases, the authorities can accept a request from their counterparts via mail/fax, which cannot be evaluated as secure gateways, or through Interpol.

(d) Competent authorities have processes in place to assess and prioritise requests and ensure that timely assistance is provided in relation to all information channels. Requests received via the Interpol channel SPOC and the SIRENE channel SPOC are processed according to rules set by the NCB Service standards and the SIRENE Manual respectively. In fact, all requests received through information channels, including national correspondence are monitored by officers of Front Office shift. In general terms, incoming requests are prioritised on a case by case basis, depending on their nature, the severity of the underlying crime, the complexity of the case and the applied measures of constraint in the requesting state.

(e) Art. 48 (par.4) of the AML/CFT law provides for the protection of information received by supervisory authorities, including information obtained from their foreign counterparts. All information kept in the MLPB IT systems is restricted. Also, Art.198[1] of the CC provides for community service, a fine, arrest or custodial sentence for a term of up to two years to those who illegally access the whole or any part of an information system. The authorities have also provided as an example the 2015 Agreement with the Government of Georgia on Cooperation in Crime Combating; and the 2001 Agreement with the Government of the Federal Republic of Germany on Cooperation in Combating Organised Crime, Terrorism and other Serious Crimes, which have provisions relating to confidentiality, and the information received. Clear processes for safeguarding the information received are also established by the PGO Order No.I-10 (15 January 2018) on the Approval of the Rules on Handling of Person's Data within the Prosecution Office; and the PGO Order No.I-71 (6 March 2015) on the Approval of Exchange of Information and Direct Consultations with other competent institutions of the EU MS. The Criminal Police Bureau safeguards all information received from foreign LEAs, including documents, in International Liaison Office Information system (TRV IS). The Order No. 35-V-100 on TRV IS of the Head of the Lithuanian Criminal Police Bureau sets procedures, requirements and restrictions of access to the system.

365. *Criterion* 40.3 – Competent authorities have a range of bilateral and multilateral agreements and MOUs to facilitate co-operation with foreign counterparts. When required, the Lithuanian authorities can establish promptly such agreements with their foreign counterparts. The Lithuanian FIU may exchange information pursuant to the provisions of the AML/CFT Law (Art. 5, par.1(6))and without the need of a memorandum of understanding. The Lithuanian FIU has entered into 14 such information exchange agreements with the FIUs of the following countries: Latvia, Poland, Ukraine, Italy, Portugal, Estonia, Belgium, Czech Republic, Finland, Croatia, Bulgaria, Slovenia, Serbia and the Russian Federation.

366. The BoL has also singed a number of MoUs on information exchange with its foreign counterparts (see C.40.12), although a MoU is not a pre-condition to information exchange. Art. 47^4 of the Law on the Bank of Lithuania provides that the BoL shall cooperate, exchange information and have the right to enter into agreements with the widest range of foreign counterparts.

367. As regards the PGO, it has signed a Memorandum of Understanding for Cooperation with the Office of the Chief Prosecutor of Georgia on 17 July 2017. A framework agreement between the PGO and the Academy of European Law has also been signed on 26 October 2017.

368. In 2014, the GCA, signed a cooperation agreement with the Lotteries and Gambling Supervisory Inspection of Latvia and the Estonian Tax and Customs Board. A cooperation agreement with the gambling regulatory authorities of the EEA was also signed in 2015. In addition, the GCA is a member of the Expert Group on Gambling Services in Brussels and participates at the EC level meetings in relation to the new EU rules in fighting ML/FT.

369. *Criterion* 40.4 – Competent authorities are able to provide timely feedback upon request to foreign authorities who have provided assistance, though not on a systematic basis. In general, feedback is provided by all competent authorities upon request. The FIU annually provides feedback to its Latvian counterpart based on a feedback list sent by the latter. The PGO utilises international liaison officers for this purpose.

370. *Criterion 40.5* – The Lithuanian legislation does not impose any of the restrictions mentioned under (a) to (d). The evaluators were advised that the Lithuanian authorities cannot refuse the request for information from foreign counterparts on the ground that it is considered to involve fiscal matters, as well as do not refuse to execute requests for cooperation on the ground of legal acts that would impose secrecy or confidentiality requirements (Art. 55(6) of the Law on Banks). There are no provisions prohibiting or unreasonably and unduly restricting the provision of assistance in case of an on-going enquiry or investigation (Art. 177 of the CPC). The only condition for an execution of assistance is that the content of the request does not conflict with human rights, Lithuania's international obligations, its legal order and does not harm the sovereignty and security of the country. The GPO informed that when it comes to requests, the execution of which is not within its competence, it re-forwards them to the competent national authority and informs the initiator of the request respectively. As regards the Criminal Police Bureau, it addresses requests of civil, administrative or law enforcement nature received to the competent authorities.

371. *Criterion* 40.6 – According to the information provided all requests from counterparts can be used only for the purposes of the criminal case, in which the assistance was requested. Competent authorities do not have law or guidance establishing controls and safeguards, but rely on standards set by relevant international bodies or arrangements (Council of Europe Convention on Laundering, Search, Seizure and Confiscation of the Proceeds from Crime and on the Financing of Terrorism (CETS 198), Art. 46(7); International Organisation of Securities Commissions Multilateral MOU (IOSCO MMOU), para.10; Europol Codes; Art. 26 of the OECD Model Tax Convention; etc.). Information is only used for the specified purpose or with the consent of the requested country.

372. According to Art. 17 of Law on Intelligence, intelligence institutions should use intelligence information solely to implement the tasks assigned thereto and only for the purposes for which it has been collected. In addition, Articles 22 and 24 of the Law provide for internal control of the intelligence institution and government scrutiny of intelligence institutions.

373. *Criterion 40.7* – The legal acts (e.g. Law on State and Official Secret, Law on the Bank of Lithuania, Law on Banks, Law on Insurance) provide requirements in order to ensure that the information received by the supervisory authorities is used only in an authorised manner (in line with the Lithuanian privacy, confidentiality and data protection measures).

374. Art. 23 and 32 of the AML/CFT Law establish that information specified in the Law and received by the FCIS may not be published or transferred to other state governance, control or law enforcement institutions and other persons, except in the cases established by this Law and other laws. The breach of this duty shall be held liable in accordance with the procedure established by laws. Also Art. 48(5(3)) of the AML/CFT law grants the right to competent authorities to refuse to provided information if the requesting authority of a third country cannot protect the information effectively.

375. *Criterion 40.8* – Competent authorities are able to conduct inquiries on behalf of foreign counterparts and exchange information which is domestically obtainable (Art. 97 of the CPC, Art. 69 of the Law on Banks, Art. 75(3) of the Law on Markets in Financial Instruments, Art. 26(6) of the Law on Payment Institutions, Art. 32(6) of the Electronic Money and EMIs, Art. 22(6)of the AML Law, Art. 30 (4)(5)(6) of the Law on Insurance, Resolution No.633 of the Government of Lithuania (17 June 2009) and Art. 19 of the Law on Criminal intelligence).

376. *Criterion 40.9* – Pursuant to Art. 5(1, point6) of the AML/CFT Law, the FIU can cooperate and exchange information with foreign institutions and international organisations in implementing AML/CFT measures.

377. *Criterion 40.10* – As a member of Egmont Group, the FIU has the obligation to provide such feedback in accordance with Cls. 19 of the Egmont group Principles for Information Exchange. The also FIU uses the PGO's International Liaison Officers to facilitate the provision of feedback.

378. *Criterion 40.11* – There does not seem to be any limitation to the type of information the FIU can exchange under Art. 5 of the AML/CFT Law. The FIU can use all its investigative powers to provide, directly or indirectly, the information from databases it has access to, including information of a confidential nature. The FIU can request information from reporting entities on the basis of a request from a foreign FIU.

379. *Criterion 40.12* – The BoL and the FIU have a legal basis for providing co-operation to their foreign counterparts, including exchanging supervisory information relevant to AML/CFT purposes. Such co-operation is permitted under the AML/CFT law (Art. 8 (par.2) and Art. 5 (par.4 and 6)), as well as under multilateral or bilateral agreements.

380. The Lithuanian authorities report that the BoL has also established international co-operation through:

i. Bilateral agreements for the mutual mixed-purposed questions with the Central Bank of Russian Federation, the Central Bank of the Republic of Belarus, the Central Bank of the Republic of Uzbekistan, the European Payments Council, the European Commission, the Central Bank of Estonia;

ii. Multilateral agreement with the Central Banks, the Supervisory Institutions and the Ministries of Finance of 25 EU Member States;

iii. Agreements with international and European Union institutions such as European Banking Authority (EBA), European Security and Market Authority (ESMA), European Insurance and

Occupations Pensions Authority (EIOPA) and International Organisation of Securities Commissions (IOSCO); and

iv. Memorandums of Understanding (MoUs):

   a. 4.1. on Cooperation and Coordination on cross-border financial stability between relevant Ministries, Central Banks, Financial Supervisory Authorities and Resolution Authorities of Denmark, Estonia, Finland, Iceland, Latvia, Lithuania, Norway and Sweden;

   b. 4.2. on prudential supervision of significant branches in Sweden, Norway, Denmark and Finland;

   c. 4.3. with National bank of Moldova;

   d. 4.4. between the Bank of Lithuania and the National Bank of the Republic of Belarus;

   e. 4.5. between the Bank of Lithuania and the Bundesaufsichtsamt für das Kreditwesen (Supervisory Institution of the Federal Banking of Germany) on co-operation in the area of supervision of credit institutions.

381. As regards international cooperation on supervisory related issues (including information sharing), the BoL has signed bilateral agreements with the Supervisory Institutions of the Republic of Denmark (10/20/2003), the Republic of Georgia (03/27/2009), the Republic of Kazakhstan (10/26/2009), the Central Bank of Cyprus, the Supervisory Institutions of the Stock exchanges of the People's Republic of China (09/13/2013), the Republic of Poland (03/01/2002), the Republic of France (10/09/2000), the Republic of Romania (11/15/2004), and the Republic of Ukraine (06/01/2010).

382. In addition, Art. 43(7) of the Law on the BoL provides for the information received for supervisory or AML/CFT purposes.

383. *Criterion 40.13* – The BoL and the FIU are able to exchange domestically-available information with foreign counterparts, including information held by FIs, provided sharing is proportionate and appropriate ((Art. 8 (par.2) and Art. 5 (par.4 and 6)). Also, Art. 43(7) of the Law on the BoL provides for the exchange of information domestically available for supervisory or AML/CFT purposes. Art. 65(6)(7) of the Law on Banks gives supervisors the right to send the information obtained for supervision purposes to the central banks of the European System of Central Banks as well as to other institutions performing similar functions.

384. *Criterion 40.14* – As mentioned in C.40.12 the BoL and FIU can exchange any information they hold (including regulatory information, prudential information, and AML/CFT information) with relevant authorities provided the disclosure is relevant to the functions of the foreign authority or where relevant to prevent or detect ML and FT (Art. 59.8 and Art. 65 (6)(7) of the Law on Banks and AML/CFT law (Art. 8 (par.2) and Art. 5 (par.4 and 6)).

385. *Criterion 40.15* – The BoL and the FIU are able to exercise domestic powers and conduct inquiries on behalf of foreign counterparts, including conducting an investigation and obtaining information or documents (Art. 69(7) of the Law on Banks, Art. 75(3) of the Law on Markets in Financial Instruments, Art. 26(6) of the Law on Payment Institutions, Art. 32(6) of the Electronic Money and EMIs and Art. 30 (4)(5)(6) of the Law on Insurance).

386. *Criterion 40.16* – Art. 48(4) of the AML/CFT law, Art. 65(9) of the Law on Banks, Art. 76(3) of the Law on the Markets of Financial Instruments, Art. 203(9) of the Law on Insurance, Art. 29 of the Law on Electronic Money and EMIs and Art. 23 of the Law on PIs requires prior authorisation of the requested party for the dissemination of information exchanged, unless the requesting supervisor is under the obligation to disclose or report such information. As regards, requests made within the IOSCO framework, the BoL acts in accordance with the IOSCO MMOU (par.10). Requirements for cooperation with other supervisory authorities are also established under respective MoUs (e.g. MoU with the Central Bank of Estonia (par.7)).

387. *Criterion 40.17* – Provisions of the CPC (Art. 68^1), provide grounds for the PGO to establish the arrangements for the exchange of information and for direct consultations with the competent authorities of other EU Member States. In addition, the Resolution No.633 of the Government of the Republic of Lithuania (17 June 2009) sets rules on the exchange of information between the Lithuanian LEAs and their EU counterparts. The Criminal Police Bureau is able to exchange domestically available information with foreign counterparts for intelligence or investigative purposes relating to ML, FT and associated predicate offences, including the identification and tracing of proceeds and instrumentalities of crime (Art. 19 of the Police Law on Criminal Intelligence).

388. Lithuanian Liaison Officers of the Police co-operate and keep close contact with liaison officers from Belgium, Israel, Japan, the United States of America, Canada, France, Finland, the United Kingdom, Germany and Spain. Liaison officers significantly facilitate information exchange, planning of joint operations and conducting other relevant actions needed for investigation, disclosure, clearance and suppression of crimes, especially those related to organised crime and terrorism.

389. *Criterion 40.18* – LEAs are able to conduct inquiries and use domestically-available, non-coercive powers and investigative techniques to conduct inquiries and obtain information on behalf of foreign counterparts. Co-operation occurs mostly through EU and Egmont mechanisms. Police co-operation takes place particularly within the framework of conventions and agreements signed by Interpol, Europol or Eurojust and bilateral agreements with EU and third countries.

390. *Criterion 40.19* – Pursuant to the PG's Recommendations on JIT (Sections II and III), teams may be formed from the officials of the institutions of EU Member States or any other States, and the officials of the bodies established under the Treaty on the EU under the lead of the prosecutor of the Prosecutor's Office of Lithuania.

391. *Criterion 40.20* – In accordance with Art.5(par.1(6)) of the AML/CFT Law, the FCIS can exchange information with "institutions of foreign states" implementing ML/FT prevention measures. Also, par.1(4) of the same article provides that the FCIS can forward information about the possible criminal act or established indications of breaches of legal acts, collected during the analysis of the information received on the basis of this Law, to the competent state or foreign institutions, provide information about the monetary operations and transactions carried out by the customer to tax administration, law enforcement and other state institutions. The authorities confirmed that this provision is understood broadly, including all authorities involved in the AML/CFT framework. In the same line, Art. 8(2) of the AML/CFT law provides that the BoL, the Department of Cultural Heritage Protection, the GCA, the Lithuanian Bar Association, the Lithuanian Chamber of Notaries, the Lithuanian Chamber of Auditors, the Chamber of Judicial Officers of Lithuania and the LAO can cooperate and exchange information with foreign institutions implementing ML and/or FT prevention measures. As regards the Criminal Police, there is no legal provision prohibiting it from exchanging information with non-counterparts.

Weighting and Conclusion

392. All agencies have the powers and abilities to provide a wide range of international assistance. There is no explicit legal provision to provide assistance rapidly. The provision of feedback is not systematic and is inconsistent across agencies, including the FIU. There is no explicit legal provision which allows competent authorities to exchange information indirectly with non-counterparts. **R.40 is rated LC.**

Summary of Technical Compliance – Key Deficiencies

Compliance with FATF Recommendations		
Recommendation	**Rating**	**Factor(s) underlying the rating**
1. Assessing risks & applying a risk-based approach	PC	• It is not clear that Lithuania has identified and assessed all of the major ML/FT risks as noted under IO 1. • It is not clear how well Lithuania was able to allocate resources and implement measures to prevent or mitigate ML/FT. • The deficiencies under R. 26 and 28 have an impact on Lithuania's compliance with this criterion. • The AML/CFT does not specify that risk assessments must be documented, that all relevant risk factors should be considered or that assessments should be kept up-to-date. • There are no appropriate mechanisms in place for the provision of information to competent authorities.
2. National cooperation and coordination	PC	• Lithuania does not have a national AML/CFT policy. • There are no co-operation and co-ordination mechanisms in place to combat PF.
3. Money laundering offence	LC	• There are minor deficiencies in relation to the criminalisation of the ML offence.
4. Confiscation and provisional measures	LC	• No measures appear to have been taken to rectify the minor gap concerning the period of validity of a restraint order. • It is not clear whether provisional measures can be made without prior notice in all cases.
5. Terrorist financing offence	LC	• There are minor deficiencies in relation to the criminalisation of the FT offence.
6. Targeted financial sanctions related to terrorism & TF	PC	• There appears to be no internal regulations within the MFA which specifically set out this responsibility. • The SSD actively monitors the territory of Lithuania to identify persons with links to terrorism or FT. However, it appeared that the SSD was not aware of the obligation to identify targets based on the designation criteria set out in the relevant UNSCRs. • Lithuania has no mechanisms and procedures in place to comply with these requirements. • There is no requirement that a prompt determination is made. • It is not clear what happens with respect to requests received by Lithuania. • There is no procedure detailing steps to be taken in cases where Lithuania makes a request to another country for listing. • The implementation of TFS set out under UNSCRs 1267/1989 and 1988 into the EU framework does not take place 'without delay', since there is a delay between the designation decision taken by the UNSC and its transposition into the EU framework. • It is doubtful whether, in practice, the freezing action takes place without prior notice. • There are no other communication mechanisms in place, except for periodic notices circulated by the FIU, which do not fulfil the requirement that updates are communicated immediately. • No guidance has been issued. Lithuania has not, however, decided that, as a rule, its citizens or residents should address their de-listing requests directly to the Focal Point through a declaration addressed to the Chairman of the Committee.

Compliance with FATF Recommendations		
Recommendation	**Rating**	**Factor(s) underlying the rating**
		• There are no procedures fulfilling these requirements.
7. Targeted financial sanctions related to proliferation	PC	• There are delays in the transposition into European law of UN decisions on DPRK, which is mitigated by the significant number of other designations by the EU. • Shortcomings noted under C.6.5 impact C.7.2.
8. Non-profit organisations	LC	• Lithuania has not reviewed the adequacy of its measures that relate to the subset of the NPO sector that may be abused for FT support. • No specific outreach to NPOs and donors in relation to FT has taken place. • The NPOs sector has not been involved in any activity to develop and refine best practices to address FT risk and vulnerabilities. • There is no legal requirement or public policy paper encouraging NPOs to conduct their transactions via regulated financial channels. • Beyond the FCIS List, trainings or education activities to update and enrich the expertise of all those involved in FT-related NPO investigations are very rare.
9. Financial institution secrecy laws	C	
10. Customer due diligence	LC	• The definition of monetary operations exempts payments to state and municipal institutions, other budgetary institutions, the BoL, state or municipal funds, foreign diplomatic missions or consular posts or settlement with these entities. • The definition of customer excludes State and municipal institutions, other budgetary institutions, the BoL, state or municipal funds, foreign diplomatic missions or consular posts. • There are no provisions related to the identification of representatives of legal arrangements. • There are no obligations to understand the ownership or control structure of legal arrangements. • There are no specific requirements related to the identification and verification for customers who are legal arrangements. • The requested information for the identification of the director of a legal person does not include the powers that regulate and bind the legal person. • Subcriterion 10.14(b) is not met.
11. Record keeping	C	
12. Politically exposed persons	C	
13. Correspondent banking	LC	• Correspondent banking relationships within the EEA are not treated as cross-border.
14. Money or value transfer services	LC	• PSPs mentioned in Art. 6(4), (5) and (6) may provide payment services without a license.
15. New technologies	C	
16. Wire transfers	LC	• C.16.16 is not met in relation to post transfers.
17. Reliance on third parties	C	

Compliance with FATF Recommendations		
Recommendation	**Rating**	**Factor(s) underlying the rating**
18. Internal controls and foreign branches and subsidiaries	LC	• It is unclear what type of information is allowed for "disclosure". • There is no requirement on the provision of group-level compliance, audit, and/or AML/CFT functions, of customer, account, and transaction information from branches, if necessary.
19. Higher-risk countries	LC	• There is no specific provision in the AML/CFT on countermeasures. • Lithuania cannot apply countermeasures independently of any call by the FATF (or the EC).
20. Reporting of suspicious transaction	LC	• The wording (Art. 16(1) of the AML/CFT law) limits the reporting in case of FT to "support" of terrorists or terrorist organisations, and is more restrictive than the Standard which refers to "FT" in general.
21. Tipping-off and confidentiality	C	
22. DNFBPs: Customer due diligence	LC	• The requirement for lawyers, notaries, other independent legal professions and accountants to comply with the CDD requirements set out in Recommendation 10 is not covered in relation to buying and selling of business entities.
23. DNFBPs: Other measures	LC	• The deficiencies identified under the Recommendation 18 and 19 impact the requirements in C.23.2 and 3.
24. Transparency and beneficial ownership of legal persons	PC	• There is no direct data available with regard to the beneficial owners of the different types of Lithuanian legal persons. • JADIS does not contain information on shareholders of some types of legal persons. • Lithuania did not assess the ML/FT risks posed by the different types of legal persons that can be created in the country. • No information has been provided to the evaluation team on C.24.4. • There is no Authority responsible for verifying the update of the information disclosed to the Register by legal persons. • The requirement under C.24.5 in relation to shareholder information applies only to some legal persons. • C24.8 is not met. • It is not clear how long legal persons are required to retain basic and beneficial ownership information. • There are no mechanisms in place to ensure that nominee shares and nominee directors are not misused for ML/FT. • The range of the monetary fine is neither proportionate nor dissuasive. • The Centre of Register indicated that no sanctions have been applied yet in cases foreseen by the law. • Lithuania does not have any mechanism in place which would monitor the quality of assistance rendered from other countries and related to exchange of BO information.
25. Transparency and beneficial ownership of legal arrangements	LC	• There are no measures in place to ensure that trustees disclose their status to FIs and DNFBPs when forming a business relationship above the threshold or carrying out an occasional transaction. • The range of the monetary fine available for legal arrangements is neither proportionate nor dissuasive when they fail to meet the requirements for timely submission or for submission of false data, documents and other requested information to the RLE and/or JADIS.
26. Regulation and supervision of	PC	• The extensiveness of the requirements to prevent criminals from involvement with control of FIs is not clear.

Compliance with FATF Recommendations		
Recommendation	**Rating**	**Factor(s) underlying the rating**
financial institutions		• A series of BoL written policies and procedures documents combine to produce a programme of supervision predicated on prudential rather than on AML/CFT supervision. • The Risk-Based System Concept the BoL attributes FIs to four sectoral categories with the aim of distributing overall supervisory resources so as to pay more attention to the largest market participants whose activities are potentially (but not necessarily) subject to higher ML risks. • The approach to assessing risk and forming conclusions on the AML/CFT risk of FIs is not articulated in writing.
27. Powers of supervisors	C	
28. Regulation and supervision of DNFBPs	PC	• A registration framework for TCSPs, accountants and real estate agents is not in place. • While there are statutory powers to prevent criminal control of DNFBPs, the coverage of this is not clear except in relation to advocates. • The Bar Association and the Chamber of Notaries do not have complete statutory powers in relation to supervision and sanctions. • Associates of criminals are not covered. • There are gaps in relation to risk sensitive supervision.
29. Financial intelligence units	LC	• Some strategic analysis is also carried out, although not in a systematic fashion. • The FIU has functions which are distinct from those of the FCIS, as a matter of formality, it is the Head of the FCIS which signs off requests for information and reports disseminated to LEAs.
30. Responsibilities of law enforcement and investigative authorities	C	
31. Powers of law enforcement and investigative authorities	LC	• It is not clear whether competent authorities can identify assets without prior notification to the owner.
32. Cash couriers	PC	• No requirements apply to mail and cargo. • Customs does not have the authority to request and obtain further information where a false declaration or disclosure, or failure to declare, has been detected. • No information was provided co-ordination mechanisms among customs, immigration and other related authorities. • There is no power to stop or restrain currency for a reasonable period of time in order to ascertain whether evidence of ML/FT may be found where there is a suspicion of ML/FT or predicate offences or when there is a false/non-declaration/disclosure.
33. Statistics	LC	• MLA requests are not categorised per legal qualification.
34. Guidance and feedback	LC	• Feedback by the FIU is not comprehensive. • While there are no requirements/procedures for supervisory authorities to provide guidance, guidance is provided in practice, particularly but not limited to banks.
35. Sanctions	LC	• The supervisory authorities for advocates and notaries do not have power to impose fines for AML/CFT breaches.

Compliance with FATF Recommendations		
Recommendation	**Rating**	**Factor(s) underlying the rating**
		• While there are fines for breaches by senior managers/directors, the maximum levels are not dissuasive. • While sanctions are applicable, in the absence of criminal penalties the sanctions framework for reporting suspicion and tipping off is not fully dissuasive.
36. International instruments	C	
37. Mutual legal assistance	LC	• There is no legal provision to provide assistance rapidly. • Some minor gaps under C.3.1 and C.5.1 impact criteria 37.6 and 7.
38. Mutual legal assistance: freezing and confiscation	LC	• Minor deficiencies under C.3.1, C.5.1 and R.37 impact Lithuania's ability to take expeditious action in response to requests by foreign countries. • The Resolution No.219 does not regulate the sharing of other types of property. • No information was provided on asset-sharing with non-EU countries or on asset-sharing when confiscation is indirectly a result of co-ordinated law enforcement actions.
39. Extradition	LC	• Some minor weaknesses relating to ML/FT offences may impact on the scope of application of extradition. • There are no clear processes for timely execution of extradition requests.
40. Other forms of international cooperation	LC	• There does not seem to be an explicit obligation to provide cooperation "rapidly". • The provision of feedback is not systematic and is inconsistent across agencies, including the FIU. • There is no explicit legal provision which allows competent authorities to exchange information indirectly with non-counterparts.

GLOSSARY OF ACRONYMS

AML/CFT	Anti-Money Laundering/Combating Financing of Terrorism
ARO	Asset Recovery Office
BNIs	Bearer Negotiable Instruments
BOs	Beneficial Owners
BoL	Bank of Lithuania
CA	Customs Authority
CC	Criminal Code of Lithuania
CDD	Customer Due Diligence
CoE	Council of Europe
CPC	Code of Criminal Procedure of Lithuania
CSPs	Company Service Providers
DNFBPs	Designated Non-Financial Businesses and Professions
DPMS	Dealers in Precious Metals and Stones
EC	European Commission
EDD	Enhanced Due Diligence
EMIs	Electronic Money Institutions
EU	European Union
FATF	Financial Action Task Force
FIs	Financial Institutions
FIU	Financial Crime Investigation Unit
JADIS	Information System of Members of Legal Persons
LEAs	Law Enforcement Agencies
LAO	Lithuanian Assay Office
MoE	Ministry of Economy
MER	Mutual Evaluation Report
MFA	Ministry of Foreign Affairs
ML	Money Laundering
MLA	Mutual Legal Assistance
MoF	Ministry of Finance of Lithuania
MoI	Ministry of Interior

MoJ	Ministry of Justice
MVTS	Money or Value Transfer Services
NBFIs	Non-Banking Financial Institutions
NPOs	Non-Profit Organisations
NRA	National Risk Assessment
PEPs	Politically Exposed Persons
PF	Proliferation Financing
PGO	Prosecutor General's Office of Lithuania
RBA	Risk-Based Approach
REs	Reporting Entities
RMSs	Risk Management Systems
SAR	Suspicious Activity Report
SSD	State Security Department
STI	State Tax Inspectorate
STR	Suspicious Transaction Report
FT	Terrorist Financing
TFC	Terrorist Financing Convention
TFS	Targeted financial sanctions
UBO	Ultimate Beneficiary Owner
VC	Vienna Convention
WG	Working Group
WMDs	Weapons of Mass Destruction

www.coe.int/MONEYVAL

December 2018

Anti-money laundering and counter-terrorism financing measures

Lithuania

Fifth Round Mutual Evaluation Report

This report provides a summary of AML/CFT measures in place in Lithuania as at the date of the on-site visit (7 to 19 May 2018). It analyses the level of compliance with the FATF 40 Recommendations and the level of effectiveness of Lithuania's AML/CFT system, and provides recommendations on how the system could be strengthened.