REINFORCING MONEY LAUNDERING RISK MITIGATION IN LITHUANIA[1]

A. Introduction

1. After a past shock that led to a reduction in transnational banking transactions, Lithuania's financial sector has readjusted to serving non-residents, posing higher money laundering risk, mostly through Fintech companies.[2] The non-resident activity in Lithuania has decreased significantly following the financial integrity breaches at Snoras and Ukio banks that lost their licenses in 2011 and 2013, respectively, with involvement of the latter in the "laundromat" operations where Lithuania was used as a transit point for suspicious transactions allegedly linked to foreign criminal activity.[3, 4] Subsequently, the BoL focused its monitoring on daily non-resident deposits and transactions in Lithuanian banks. Due to the recent growth of the fintech hub, Lithuania's financial sector's focus shifted away from bank-centric focus on servicing domestic market to facilitation of cross-border payments, with most transactions conducted by non-residents with origination and destination outside Lithuania, including higher Money Laundering and Terrorism Financing (ML/TF) risk countries.[5] Fintech developments have impacted the financial sector and risk profile of the country, challenging the authorities' resources and capacity to mitigate the ML/TF risks.

2. The rapid expansion of the fintech sector in Lithuania has increased the transnational illicit financial flows risks facing the country. Growth of Lithuania's Fintech hub gained momentum after the adoption of a Fintech Strategy in 2016, which was led by the Ministry of Finance and adopted to diversify the financial sector and promote development of the financial ecosystem by providing accommodative regulatory, tax, and policy environment. The number of fintech companies in Lithuania has more than tripled since then—from 82 at the end of 2016 to 265 at the end of 2021, with Lithuania becoming the European Union (EU) leader by the number of licenses issued to payments and electronic money institutions. This expansion was facilitated by enabling payment service providers and other non-bank financial institutions (including those that are licensed in other European Economic Area countries) to use the BoL payment system CENTROlink for access to Single Euro Payments Area infrastructure. Total value of payment transactions conducted by electronic money institutions (EMIs) and payment institutions (PIs) increased by 3.8 times in 2021 and amounted to EUR

[1] Written by Maksym Markevych with contributions from Grace Jackson, Alexander Malden, and Santiago Texidor. The paper is also informed by the ongoing regional IMF Nordic-Baltic Capacity Development Project that focuses on analysis of cross-border ML/TF threat and related aspects of banking sector supervision.

[2] The Fintech Landscape in Lithuania 2021–2022

[3] The Bank of Lithuania revoked the licence of AB bankas SNORAS and will apply to court regarding bankruptcy | Bank of Lithuania (lb.lt)

[4] https://www.lb.lt/en/news/the-bank-of-lithuania-will-apply-to-court-on-initiation-of-bankruptcy-proceedings-against-ukio-bankas

[5] Higher ML/TF risk countries include countries with a higher rate of economic crimes, tax practices that may be vulnerable to tax evasion (e.g., not cooperating internationally on tax matters), offshore financial centers, countries posing higher risk for use of funds for terrorism. This also includes countries under the increased FATF monitoring and the EU list of high-risk third countries

195 billion. In June 2021 the BoL revoked license of a fintech company for severe infringements of AML/CFT requirements based on the results of an inspection that was triggered by the announcement of German Federal Financial Supervisory Authority regarding their supervised entity.[6, 7] In addition to the fintech companies mentioned above, Lithuania's light registration regime for virtual asset service providers (VASPs) involves a low level of entry checks/requirements and has attracted numerous entrants, mostly during the last year, bringing the number of VASPs registered in Lithuania to 407.

3. This paper analyses selected aspects of Lithuanian anti-money laundering and counter-terrorist financing (AML/CFT) regime, focusing on financial integrity implications of growing fintech industry that relies heavily on non-residents and cross-border activity. The paper describes various indicators of increasing cross-border ML/TF threats, analyses aspects of risk-based approach to supervision of financial sector, with a focus on PIs and EMIs, authorization and supervision of VASPs conducted by FIU, and access and oversight of the BoL payment system CENTROlink. The paper does not aim at assessing the compliance of the overall AML/CFT regime with the Financial Action Task Force (FATF) international standards, which was done by MONEYVAL[8] in 2018.[9]

B. Increasing Cross-Border ML/TF Threats

4. The number of fintech companies has grown rapidly in Lithuania, driven mostly by the entry of electronic money and payments institutions with a focus on cross-border payments. The number of fintech companies has more than quadrupled from 55 in 2014 to 265 in 2021 (Figure 1). Many of the Lithuanian fintech companies—for example, working in the areas of financial software, data analytics, compliance management, and cybersecurity—do not face ML/TF risks and are not subject to AML/CFT requirements. Out of 265 fintech companies, 147 are licensed as EMIs, PIs or specialized banks. Cross-border payments emerged as the main area of focus and specialization of the Lithuanian fintech hub with the majority of fintechs providing cross-border payment services, online foreign exchange, online payments, and e-commerce transactions. Around 60 percent of fintechs have their headquarters in Lithuania, while the remaining 40 percent mainly focus on non-EU markets, with nearly 70 percent of their core operations outside of the EU.[10]

[6] https://www.lb.lt/en/news/licence-of-finolita-unio-revoked

[7] The BoL has also revoked license of another EMI in 2021: https://www.lb.lt/en/news/the-licence-of-uab-epayblock-revoked-due-to-gross-breaches-of-anti-money-laundering-requirements. Additionally in 2021, the BoL has temporarily restricted activities of 4 financial institutions (3 EMIs, 1 specialized bank).

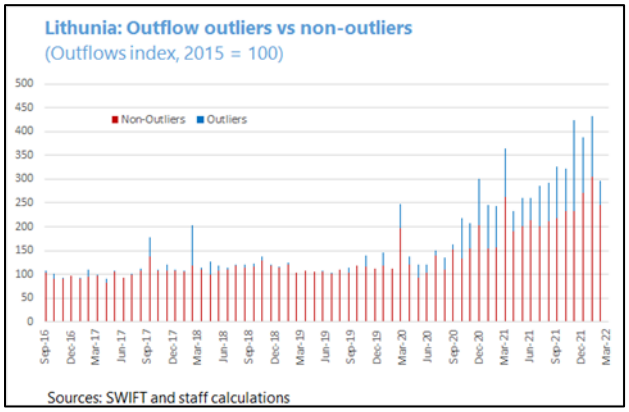
[8] The Council of Europe's Committee of Experts on the Evaluation of Anti-Money Laundering Measures and the Financing of Terrorism.

[9] The MONEYVAL assessment rated Lithuania's AML/CFT regime as insufficiently effective in ten out of eleven pillars of an effective system, including moderate effectiveness of AML/CFT supervision, preventive measures by reporting entities, and ML/TF risk understanding and domestic coordination. Given the results of the assessment, Lithuania was placed in an enhanced follow-up process. Following the MONEYVAL assessment Lithuania has strengthened its legislative and regulatory framework and took steps to enhance its AML/CFT effectiveness. Lithuania achieved full compliance with eight of the forty FATF Recommendations focused on technical compliance issues, retains minor deficiencies in adoption of 25 recommendations (rated largely compliant), partial compliance with seven recommendations and no non-compliant ratings.

[10] The Fintech Landscape in Lithuania 2021–2022

5. Due to the focus of new financial sector entrants on payments services, the volume and value of cross-border payments have grown strongly and at a faster rate with higher risk countries. Total value of payment transactions conducted by EMIs and PIs increased by 3.8 times in 2021, reaching EUR 195 billion in 2021, with one company accounting for 58 percent of this turnover.[11] Reflecting this growth, the overall inflows to and outflows from Lithuania have increased by 2.4 times in the last six months of the analysis[12] as compared to financial flows in 2015 (Figure 2). Moreover, flows with the countries that have been identified as offshore financial centers, some countries under the increased FATF monitoring, on the EU high-risk third countries, and some other higher risk countries have increased at a faster rate than the overall flows (Figure 3).[13] Based on the BoL data, while the share of non-resident deposits has tripled in a year to the first quarter of 2021, it remains low at 3.3 percent.

6. The increase in and changing pattern of cross-border payments have led to the increase in outlier activity according to the Fund's anomaly detection machine learning algorithm. The Fund developed an unsupervised machine learning algorithm[14] to monitor global financial flows to detect unusual patterns of financial flows, based on the global cross-border payments since 2013 and incorporating various indicators of lower and higher ML/TF risks.[15] The number and value of outflows-outliers have spiked since 2020 following the period of low outlier activity with majority of the recent increase in outflows from Lithuania being identified as outlier payments.



7. The increase in and changing pattern of cross-border payments have led to the increase in outlier activity according to the Fund's anomaly detection machine learning algorithm. The Fund developed an unsupervised machine learning algorithm[16] to monitor global financial flows to detect unusual patterns of financial flows, based on the global cross-border payments since 2013 and incorporating various indicators of lower and higher ML/TF risks.[17]

[11] Review of the Activities of Electronic Money and Payment Institutions, Q4:2021

[12] October 2021–March 2022

[13] The financial flows analysis presented uses payments between the customers of financial institutions (Message Type 103 and Message Type 103+ of SWIFT).

[14] Fund's cross-border payments outlier detection algorithm is based on the isolation forest approach (Fei Tony Liu, Kai Ming Ting and Zhi-Hua Zhou; 2008).

[15] These indicators include bilateral trade, portfolio, and direct investments, average transaction value, appearance of new payment corridors, strength of AML/CFT regime, financial secrecy, harmful tax practices, corruption perceptions. The payment amounts are normalized on the ordering country level.

[16] Fund's cross-border payments outlier detection algorithm is based on the isolation forest approach (Fei Tony Liu, Kai Ming Ting and Zhi-Hua Zhou; 2008).

[17] These indicators include bilateral trade, portfolio, and direct investments, average transaction value, appearance of new payment corridors, strength of AML/CFT regime, financial secrecy, harmful tax practices, corruption perceptions. The payment amounts are normalized on the ordering country level.

Figure 1. Fintechs in Lithuania

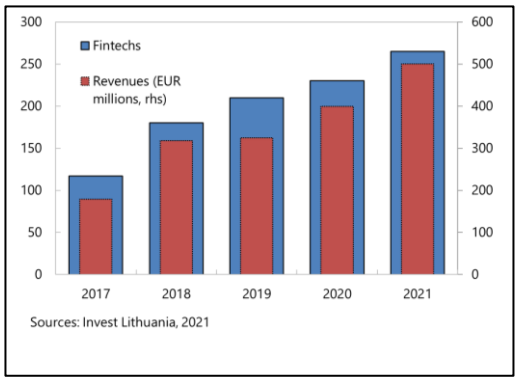


Figure 2. Gross Aggregate Cross-Border Flows

(Index, 2015=100)

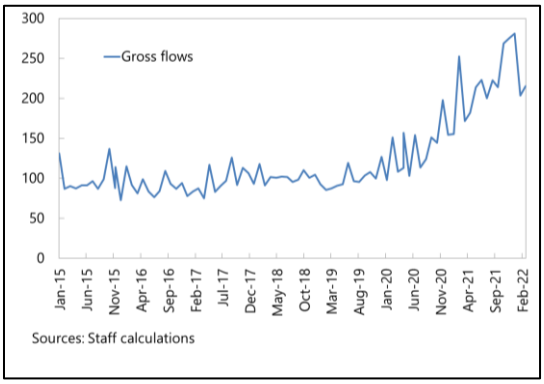


Figure 3. Gross Flows to Financial Centers

(Flows index, 2015=100; share in percent)

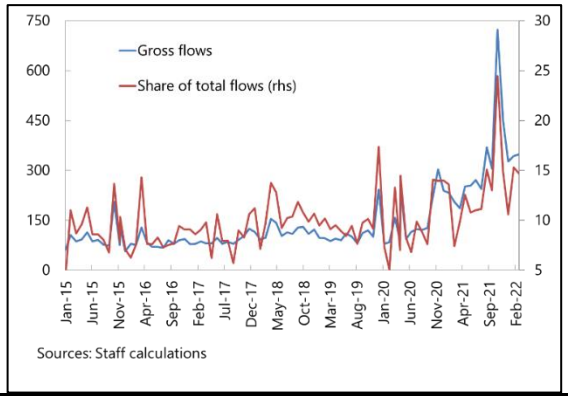
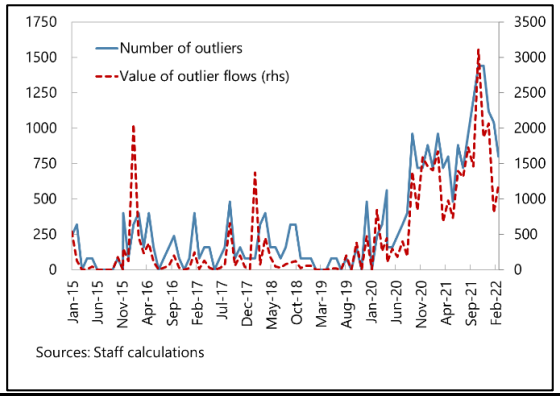


Figure 4. Outflows Outliers

(Index, 2015=100)



The number and value of outflows-outliers have spiked since 2020 following the period of low outlier activity with majority of the recent increase in outflows from Lithuania being identified as outlier payments.

C. National Understanding of Non-resident ML/TF Risks

8. The Lithuanian authorities' understanding of ML/TF risk is largely grounded in the 2019 ML/TF National Risk Assessment (NRA) that updated and expanded on the 2015 NRA. The 2019 NRA, which was published in 2020, was conducted with a view to address the deficiencies identified by MONEYVAL in the 2015 NRA. It used a more comprehensive set of information for the assessment, introduced some analysis of ML methods and trends, identifying 88 risk scenarios for 19 covered sectors based on which each sector and its products were assessed against ML and FT risks. As a result of the NRA improvements, Lithuania was re-rated to "largely compliant" with the FATF recommendation on NRAs. The 2019 NRA concluded that, among some of the sectors and products mentioned in this paper, virtual assets (VA), transfer of funds, and cash deposits to financial institution (FI) accounts face the highest ML threat (score 4), while banking (all products), currency exchange firms, investment companies, money remittances, EMI, and PI have the second highest ML threat (score 3). Assessment of ML vulnerabilities concluded that virtual currencies are the most vulnerable (score 4),

while all other products and services mentioned in the previous sentence have the second highest ML vulnerability score (3).

9. Lithuanian EMI and PI are facing elevated ML/TF inherent risk across all four classical ML/TF risk factors: customer base, delivery channels, geography of activity and services provided. Cross-border payments, the main service provided by the Lithuanian fintechs, receives particular attention in the FATF standards as higher ML/TF risk activity, with added complexity that most of the cross-border payments facilitated by the Lithuanian fintechs are not linked to Lithuania with origination and destination of transactions abroad. As the Lithuanian fintechs have business models not focused on the domestic market, the customer base of EMI and PI are mostly non-residents, in some entities close to 100 percent of their client base. Moreover, the national risk assessment (NRA) of ML/TF risks notes that a large share of customers (up to 70 percent) is from offshore countries, which also challenges FIs' understanding of purpose of business relationship and correct identification of beneficial ownership of customers that have complex corporate structures. Based on the analysis of suspicious transaction reports filed by reporting entities, the NRA mentions the trend in pass-through payments where non-residents are using the Lithuanian financial center as a transit point. It also concluded that EMI and PI are attractive for criminals as customer due diligence (CDD), in particular customer onboarding, is conducted remotely (non-face-to-face business relationships is a traditional ML/TF risk factor). Services to legal persons account for the majority of EMI and PI revenue, while services to natural persons generate 20 percent of the revenue[18] (relationships with legal persons are traditionally considered higher ML/TF risks). Moreover, some of the EMI and PI specifically focus on serving higher risk customers, such as VASPs, gambling platforms, military companies.

10. Lithuanian EMI and PI also face elevated ML/TF risk due to their ML/TF vulnerabilities. Overall, it appears that Lithuanian EMI and PI face elevated inherent risk due to non-resident customer base, non-face-to-face delivery channels, cross-border payments as the main service, wide global reach of their operations (including in higher risk countries), which is not adequately mitigated by weaker AML/CFT systems and controls. According to the NRA, as most of their customers are non-resident, including from offshore countries, the EMI and PI face difficulties in verifying the customer identity and purpose of the business relationship using reliable external sources and non-face-to-face methods. The BoL has also identified cases of incorrect customer or beneficial owner information that were attributed to the weakness of remote onboarding.[19] According to the NRA, the AML/CFT systems and controls of EMI and PI (e.g., transaction monitoring systems) are less effective than in the banking sector, including due to these institutions' recent entry and a focus on growing the customer base rather than AML/CTF regulatory compliance. The NRA also noted that EMI and PI have lower understanding and weaker controls of TF risks as compared to banking. In addition, according to the NRA,[20] most EMI and PI have not performed organization–wide ML/TF risks assessments. The NRA indicated that the rapid growth of EMI and PI institutions might create challenges for the supervisors to conduct timely on-site inspections and offsite monitoring—this conclusion reflected doubling of

[18] Invest Lithuania Fintech Survey Results, 2021

[19] Lithuanian national risk assessment of money laundering and terrorist financing

[20] While the NRA report was published in 2020, the assessment used data from 2016-2019

EMI and PI to 107 in 2019, which continued to grow strongly since then. In the BoL Risk Scoring Methodology EMI and PI are rated as a sector in the highest risk category, requiring enhanced supervisory attention.

11. The NRA methodology should strengthen analysis of ML/TF risks from non-resident activity and cross-border payments and reflect the evolution of the financial sector. The NRA has concluded that the financial sector in Lithuania is bank-centric as they hold 79 percent of the financial system assets, which appears not to take into account the importance of payment services to ML/TF risk profile of Lithuania. The NRA also notes that the banking services are mainly traditional trade financing, loans, and deposits, which can be updated to reflect the growth in the turnover and variety of products and services that are being offered in Lithuania by the high number of non-bank FIs. The NRA can also benefit from more attention to the evolved structure of the financial sector, its geographic reach, and client base. In addition, it should focus on the recent growth in the number of registered VASPs, other VA/VASP-related regulatory and legislative developments, risk assessment of various types of VA and VASP activities, and composition of the VASP sector in Lithuania. While the NRA notes that the number and value of payments is growing each year, the assessment appears to focus mostly on the stock of non-resident deposits, noting their low number in Lithuania. The NRA should incorporate an analysis of ML/TF threats inherent in cross-border payments, particularly with the higher risk countries, and of economic rationale (e.g., foreign trade, portfolio, and direct investments between the two countries) that underlies the cross-border activity. Based on this analysis the NRA can identify countries that pose higher ML/TF risk to Lithuania, which could be instrumental in more effective management of cross-border ML/TF risks, including further strengthening of risk-based approach to supervision.

12. The national understanding of TF threat focuses on the terrorist activity in Lithuania and should be developed considering Lithuania's role in facilitating cross-border payments. As no organized groups motivated by extremist ideologies with the intent and capacity to commit terrorist acts have been identified in Lithuania in recent years, the Government assessed that the level of terrorist threat is low.[21] Based on the low risk of domestic terrorist activity, the State Security Department of Lithuania concluded that the threat of TF is also low. However, the focus on domestic terrorism threat does not take into account the risks from the substantial cross-border payments in Lithuania, as its financial sector can be abused for transferring the funds intended for terrorism from donors to terrorists, both outside the country. This is a significant gap as transfers using remittances and other products of EMI/PI figure prominently in the TF typologies. In addition to introducing the analysis of TF risks from the pass-through payments, the NRA can benefit from the analysis of TF risks of raising the funds domestically for terrorism acts abroad. These analyses should leverage the analysis of cross-border payments mentioned above, notably of the links with the higher TF risk countries. Similarly, the NRA would benefit from the analysis of risks of financing of proliferation of weapons of mass destruction and effectiveness of implementation of targeted financial sanctions due to the proximity to countries with high number of sanctioned individuals and entities.

13. Considering the growing importance of payment services and non-resident business, the authorities can consider establishing a national mechanism to monitor cross-border payments.

[21] The Government of the Republic of Lithuania, Order No. 93, 2015

Considering rapid developments in the Lithuanian financial sector and that the next NRA would be prepared and published in 2024, the authorities may find useful to set up a national mechanism to monitor cross-border payments or to conduct an ad hoc thematic risk assessment. This national mechanism can incorporate various sources of data on non-resident activity, such as: aggregated data from the BoL's AML/CFT supervision division on cross-border payments, non–resident deposits and client base; BoL's payments department data on transactions through various payment infrastructures, including CENTROlink; suspicious transaction reporting to the Money Laundering Prevention Board of the Financial Crime Investigation Service[22] (Lithuanian FIU) related to non-resident activity; transactions in VAs from the reporting of VASPs; reporting on cross-border activity of taxed entities to the State Tax Administration. Such analysis would allow to develop a comprehensive and up-to-date understanding of non-resident activity in Lithuania and its ML/TF risk implications to inform high-level policy decision-making regarding calibration of jurisdictional ML/TF risk profile and risk appetite. The results of this monitoring and analysis would improve understanding of illicit financial flows risks and inform recalibration of policy priorities, including those of key AML/CFT institutions, such as Lithuanian FIU, law enforcement agencies, AML/CFT supervisors.

Recommendations:

- Expand the NRA to cover analysis of ML/TF risks from non-resident activity and cross-border payments and reflect the evolution of the financial sector
- Develop understanding of ML/TF higher-risk countries based on the Lithuania-specific risk factors
- Consider developing a national mechanism for monitoring macro-trends in cross-border financial flows

D. Enhancing Implementation of the Risk-Based Approach to AML/CFT Supervision

14. The MONEYVAL assessment—finalized before the recent growth of the Fintech sector—concluded that AML/CFT supervision is only moderately effective and major improvements are needed. The BoL is responsible for licensing and AML/CFT supervision of the financial sector in Lithuania, including fintech companies such as EMI and PI. The MONEYVAL assessors highlighted very good market entry controls to prevent criminals from holding controlling interest or a management function in an FI. The assessors also noted that the BoL 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 level of sanctions applied by the BoL has generally been commensurate with its supervisory findings, its sanctioning regime was not fully effective and dissuasive at that time. The assessment also concluded that a shortage of staff resources has had a negative impact on the overall effectiveness of the risk-based approach to supervision.

[22] Full name: Money Laundering Prevention Board of the Financial Crime Investigation Service under the Ministry of the Interior of the Republic of Lithuania

15. The BoL has made substantial progress in strengthening its AML/CFT supervision since the 2018 MONEYVAL assessment, conducting detailed off-site monitoring of ML/TF risks. In December 2020, the BoL has adopted the AML/CFT Supervision Policy and the ML/TF Risk Scoring Methodology—important steps in strengthening BoL's risk-based approach to AML/CFT supervision. The policy envisages that the frequency and scope of inspections should be based on risk and proportionality and that allocation of resources should be based on the risks of specific FI or a sector. The new methodology for ML/TF risk assessment envisages FI-specific ML/TF risk scoring, which is based on data collection and risk evaluation. Data is gathered on various risk indicators related to the FI's customer base, products/services offered, and countries of operations to generate the inherent ML/TF risk of an FI. In order to calculate the residual risk, the inherent risk ratings are combined with a score representing the strength of the FI's ML/TF systems and controls, which reflects the supervisory judgement based on the qualitative assessment of the existing controls, mitigating measures, and other factors (e.g., adverse media revelations or negative information from another authority). Based on the progress in developing risk-based approach to supervision, MONEYVAL re-rated Lithuania´s level of compliance with the FATF recommendation on regulation and supervision of FIs from "partially compliant" to "largely compliant."

16. The BoL should develop its understanding of higher-risk countries taking into account Lithuania-specific ML/TF risk factors. The BoL collects detailed statistics on the FIs' cross-border activities, with disaggregation on the individual country level, but for risk scoring of the FIs' country risk relies exclusively on the jurisdictions listed by the FATF, the European Commission and the Ministry of Finance of Lithuania.[23] Leveraging its offsite monitoring and quarterly data collection from EMI/PI, the BoL is able to react dynamically to external events and analyze ML/TF risks facing supervised entities emanating from business relationships with certain countries. Considering the criticality of cross-border activity, the BoL should develop its understanding of higher ML/TF risk countries considering the Lithuania-specific foreign ML/TF threats, potentially based on the enhanced NRA methodology as outlined above. The blanket treatment of all transactions from and to the EU, which accounts for majority of the transactions in Lithuania, as lower ML/TF risk can be nuanced to account for differences in the risk profiles of the EU countries. The BoL AML/CFT supervision may usefully distinguish between higher risk countries that provide non-transparent corporate vehicles (part of customer risk factor) and countries posing higher risk of laundering the foreign proceeds of economic crimes in or via Lithuania, or of facilitating the laundering of proceeds of crime that originate in Lithuania (part of geographical risk).

17. The Risk Scoring Methodology would benefit from incorporation of the supervised entity's size as measured by the turnover of cross-border activity. In addition to the risk assessment of cross-border payments as part of geographical risk factors, the BoL should consider introducing the overall value of EMIs and PIs payments activity as a separate risk factor directly in the Risk Scoring Methodology to ensure an appropriate focus on the institutions with material ML/TF risks. Considering the strong emphasis on cross-border services in Lithuania's financial sector, size in terms of the value and volume of cross-border transactions seems to be a more relevant ML/TF risk indicator than the FI's assets value. The methodology indicates that more intensive supervisory actions shall be

[23] This sentence refers to the jurisdictions under the FATF increased monitoring, EU high-risk third countries, and the Ministry of Finance targeted territories.

directed at larger and systemically more important institutions, which appears to reflect mostly the prudential supervisory considerations rather than ML/TF-specific considerations. In addition, all geographical risk factors used in risk rating of an institution are based on the share of the clients from the countries on the FATF/EU/Ministry of Finance lists and share of their cross-border transactions, which is important to adjust to the overall client base and cross-border transactions turnover of the supervised institution. For example, an FI with high cross-border activity may have a small share of payments with a high-risk country, but which may be nonetheless substantial in absolute numbers. The authorities can consider introducing to the risk scoring the nominal values for the number of customers from and value of transactions with higher risk countries to ensure consistency of geographical risk scoring across the institutions. Considering the resource shortage, this would also allow to prioritize the FIs with the most material high level of ML/TF risks.

18. The methodology should also incorporate ML/TF risk factors related to channels of delivery of financial products and services. While delivery channel risks are considered as part of expert assessment, where the ML/TF inherent risk score can be adjusted by one point (out of 4), the delivery channels can be usefully included as a separate risk factor group in the risk scoring model to ensure consistency in the treatment of risk related to delivery channels and formalization of the approach. Specifically, the methodology can benefit from including the share of customers that were onboarded remotely—a common onboarding method for fintech companies, which can be vulnerable to ML/TF.[24] As the BoL already collects and evaluates statistics on cash payments, cash operations, such as cash deposits or withdrawals, can be another useful risk factor to assess in a supervised entity as fintech EMI/PI are expected to conduct mostly non-cash transactions. Another delivery channel risk factor that can be considered in risk scoring of supervised EMI/PI is use of intermediaries, agents, or third parties to offer services and products.[25]

19. Customer risk grouping can be usefully expanded to focus on the specific categories of clients that pose high ML/TF risk. The methodology covers traditional types of higher risk customers: politically exposed persons, legal entities, and non-residents can benefit from including some of the sectors that pose elevated ML/TF risk to Lithuania. In particular, provision of services to VASPs and dealing in VA can be added as a risk factor. Other types of customers that can be considered for integration into the risk ratings are customers that are active in higher risk sectors, such as infrastructure, defense, financial services, real estate, extractive industries, and designated non-financial businesses or professions (DNFBPs).[26] The BoL currently collects and evaluates some data on the EMI/PI customer base: non-profit organizations, politically exposed persons, trusts, and considers expanding the data collection from the EMI/PI to include various types of higher risk customers, such as VASPs, gambling companies, financial institutions. Also, the methodology can benefit from

[24] Risks related to the remote onboarding are considered by the BoL as part of the EPI/MI sectoral risk analysis and are highlighted in the communication to the supervised entities.

[25] The BoL collects quarterly data on the activities of intermediaries that is being evaluated as part of EPI/MI sectoral analysis.

[26] DNFBP includes: Casinos; Real estate agents; Dealers in precious metals and stones; Lawyers, notaries, other independent legal professionals, and accountants; Trust and Company Service Providers.

differentiating domestic and foreign PEPs due to the different level of risk that they pose[27] also with an aim to focus supervisory efforts on improving compliance with enhanced due diligence requirements for PEPs.

20. The authorities should also strengthen the coverage of all supervised entities with data collection and risk scoring. Currently, the lower risk FIs (group 1) are subject only to ad hoc data collection, and analysis with no risk scoring, which challenges the authorities' monitoring of ML/TF risk developments in lower risk FIs and their ability to adjust the risk scoring to re-rate the FIs as higher risk to reflect increasing ML/TF risks. In addition to the BoL's monitoring of public information, it could be also useful to cover in the methodology the implications of adverse events in the operations of an FI on its risk scoring.

21. The BoL currently conducts "full-scope" AML/CFT on-site inspections with a focus on banks. During the on-site inspections, AML/CFT supervisors check FI's compliance in various fields, including implementation of internal controls, identification and assessment of ML/TF risks, identification of the customer and beneficial owner, compliance with the requirements of CDD, reporting of suspicious transactions, application of targeted financial sanctions. The focus on "full-scope" inspections is supported by the BoL detailed list of inspection criteria in various areas against which an FI should be inspected. However, the Inspection Methodology also provides for flexibility to adjust the areas covered in an inspection depending on the purpose, scope, and complexity of the specific inspection and the BoL has practical experience of conducting targeted on-site visits covering, for example, only certain aspects of customer due diligence implementation, such as ongoing monitoring and customer identification. Considering substantial non-resident risks facing FIs, supervisory attention can be required in the areas of identification of and enhanced due diligence for foreign PEPs, verification of BO of foreign legal persons with complex corporate structures, reporting of suspicious cross-border transactions. The BoL usually spends from one to two months on-site, involving two to three full-time employees. These inspections generate useful information and have successfully uncovered deficiencies in implementation of AML/CFT-related requirements but are so resource-intensive that, at the current staffing level, they effectively limit the number of FIs that can be inspected "full-scope" to a maximum of around five percent of supervised population (approximately 15 institutions). However, the reduction in the number of prospective entrants may reduce demand for the AML/CFT division's resources for licensing purposes going forward.

22. The BoL should bolster supervisory coverage of FIs, particularly by on-site inspections, with a focus on supervised entities with higher levels of activity that have not been inspected. The BoL has adopted the minimum engagement model in 2020, outlining that the highest risk institutions (group 4) should be inspected at least once in 2–3 years with a thematic analysis once in 3–5 years and annual meetings with the AML/CFT-responsible manager. Last year the BoL inspected three banks and six non-bank FIs—with this rate of on-site inspections and considering that majority of supervised population is risk group 3 or 4, half of the supervisory population can be covered in more than 15 years. Considering that the majority of the FIs operate in high ML/TF risk sectors and are

[27] The Lithuanian AML/CFT Law does not differentiate between domestic and foreign PEPs, as all PEPs are considered high risk. However, for the purposes of AML supervision it might be useful to distinguish particular types of foreign PEPs that pose particularly high ML risk.

classified as group 3 and 4, the BoL should significantly bolster the supervisory coverage of FIs to implement its minimum engagement model. Considering that majority of supervised entities are new entrants to the market and haven't been inspected,[28] an on-site inspection can be instrumental for supervisors to assess the quality of AML/CFT systems and controls of an FI and to understand its business model and implications for ML/TF risk in more detail. The three year-cycle for the highest risk FIs outlined in the BoL model may not provide sufficiently up-to-date understanding of some FIs' ML/TF risks due to the rapid evolution of fintech business models and types of products and services offered.

23. The BoL has made welcome improvements in strengthening the resources, capacity, and institutional arrangement of its AML/CFT supervision establishing a dedicated AML/CFT division. Since the MONEYVAL assessment's recommendation that all supervisory authorities should be provided with the additional budgetary and human resources, the BoL has continuously increased resources dedicated to AML/CFT supervision. The number of dedicated AML/CFT staff has increased from five in 2018, to 10 in 2020, to 13. In addition, in January 2019, the BoL changed its AML/CFT supervisory structure by establishing a separate AML unit responsible solely for AML/CFT supervision under the Financial Market Supervision Service to replace the AML/CFT division, which was part of the general operational risk division. Moreover, other BoL divisions contribute to AML/CFT efforts—Licensing division is managing the market entry process and Enforcement and Legislation division are leading on the legislative matters and enforcement measures for supervised entities, including AML/CFT.

24. However, the increase in AML/CFT resources did not keep pace with the expansion in the number of supervised entities and is not commensurate with the growing ML/TF risks. While the authorities were addressing the staff shortage identified in 2018, the number of supervised entities has grown rapidly from 130 at the start of 2018 to close to 300 currently. Moreover, the newly licensed financial institutions were mostly fintech companies with business models different from the traditional financial institutions, requiring strengthened supervisory capacity, including in financial technology, and understanding of their distinctive ML/TF risks.

25. The supervisory coverage of FIs by the BoL can be improved by increasing staffing of the AML/CFT division. The BoL should increase the AML/CFT division's resources based on the requirement of its minimum engagement model, which may include not only hiring of the staff, but also further development of the data analytics toolkit. Hiring of the new staff can be used to diversify further the skillset of AML/CFT supervisors, including in risk management, financial sector operations, fintech, and data analytics. The current plan to hire an additional supervisor falls short of filling the resource shortage. While the efforts to close the gap between the supervisory population and staffing of the AML/CFT division are ongoing, any further increases in the number of supervised entities would put additional strain on AML/CFT supervision.

26. The supervisory coverage can also be broadened by the BoL by more active use of risk-based targeted on-site inspections. Such approach would allow conducting shorter, more focused

[28] All supervised entities undergo ML/TF risk assessment during the licensing stage.

inspections targeting the aspects that pose elevated risks within an individual FI, such as particular customers, transactions, services, or compliance gaps. Targeted inspections can also focus on categories of, for example, customers, transactions, or services that pose elevated risks to the entire sector, allowing the BoL to respond more dynamically to uncovered or rapidly evolving ML/TF risks, trends, and methods. The BoL well-developed off-site monitoring and understanding of supervised entities that have already underwent full-scope inspections would allow focus on higher risk (and omit low risk) areas in an individual FI, facilitating efficiency of targeted inspections.

27. The BoL is a proactive supervisor with a continuous focus on promoting understanding by supervised entities of their obligations and ML/TF risks. The BoL organizes regular (at least quarterly) compliance meetings with the banking sector and semi-annual meetings with the EMI/PI to give an overview of ML/TF risks, legislative and regulatory developments, and discuss other AML/CFT topics. The BoL and the Ministry of Finance launched the Centre of Excellence in Anti-Money Laundering in May 2021 to combine the efforts of public and private sectors in strengthening the AML regime in Lithuania. The AML Centre of Excellence can benefit from the participation of the Lithuanian FIU, law enforcement agencies, and the State Tax Inspectorate. Notably, EMI and PI, comprising majority of the supervised population, are not members of the Centre of Excellence (although a fintech association is a participant), which is an important gap as most of these institutions are new entrants, with new business models and associated ML/TF risk, and haven't been inspected yet. The BoL has also issued various documents to promote AML/CFT compliance, such as "Updated AML/CFT Guidelines for the Financial Market Participants," "Guidance on higher risk customers and individual customer ML/TF risk assessment" and "Overview of business-wide ML/TF risk assessment" with good practices in the business risk assessment based on the analysis of risk assessment of 20 FIs.[29] In addition, the BoL routinely communicates to the CEOs of supervised entities results of its offsite monitoring and risk analysis, including recommendations on application of enhanced due diligence tailored to individual types of FI ("Dear CEO letters").

Recommendations:

- Increase the number of financial institutions subject to on-site inspections (and other bilateral supervisory engagements) each year by: (i) increasing the number of dedicated AML/CFT staff in the BoL, and (ii) more active use of risk-based targeted on-site inspections
- Strengthen BoL's understanding of ML/TF higher-risk countries and incorporate it in the institutional risk scoring matrixes, inspection activities and other elements of risk-based supervision
- Conduct thematic review of FIs' exposures to the identified higher-risk countries
- Integrate delivery channels and value and volume of conducted cross-border payments directly as a separate risk factor in risk scoring of EMIs and PIs
- Expand customer risk grouping to focus on the specific categories of clients that pose high ML/TF risk, such as VASPs

[29] Other relevant documents issued by the BoL are "Overview of monitoring of the customer's business relationship and transactions," "Guidelines for financial institutions serving customers engaged in virtual assets activity," "Overview of risk management and prevention of fraud and illegal financial services", "Guidelines for detection of shell companies,"

- Strengthen the coverage of all supervised FIs with data collection and risk scoring

E. Regulation and AML/CFT Supervision of VASPs

28. A high number of VASPs has registered over the last year in Lithuania, with VASP sector becoming a source of emerging ML/TF risk. The 2019 NRA determined the level of ML/FT risk, threat, and vulnerability of VASPs being the highest among all assessed sectors and products. Based on the NRA findings, Lithuania amended its AML/CFT law in December 2019, introducing requirements, including AML/CFT-related such as customer due diligence, transaction monitoring, for VA/VASPs, and re-allocated Lithuanian FIU resources to VASP supervision. Lithuania experienced strong influx of VASPs registering in Lithuania since October 2021, bringing the current number to high 407 registered VASPs. Reportedly, the entry of some VASPs to Lithuania was prompted by strengthening legislative and regulatory requirement for VASPs in other EU countries. The Lithuanian FIU estimates that only 25 VASPs are fully operational at the moment, noting that at least 6 months are required to fully launch VASP operations. As a result, Lithuanian VASP sector's activity may increase substantially in the short-term, with corresponding increase in associated ML/TF risks.

29. Current registration regime for VASPs imposes light requirements for VASP sector entry, however, Parliament has adopted the amendments to strengthen AML/CFT legislation for VASPs. Under the former regime, VASPs could start operating in Lithuania after registering with the Register of Legal Entities administered by the State Enterprise Centre of Registers, providing contact information of their money laundering reporting officer and attestation of understanding and compliance with AML/CFT requirements for VASPs. Considering the national understanding that VASP activity poses the highest ML/TF risk, Lithuania should strengthen VASP market entry controls. Particularly, a stronger emphasis on fitness and propriety tests appears warranted as currently only a person convicted of economic crimes cannot own or control a VASP. The Lithuanian FIU (or other VASP supervisor in the future) should examine the integrity, reputation and competence of owners and senior management of registering VASPs, including to prevent criminals from holding significant or controlling interest or a management function in a VASP. This recommendation applies to both current registration regime that allows VASPs to start operations when the required documents are submitted and to a licensing regime that the authorities may wish to consider for the largest or riskiest types of VASPs. Lithuania should also assess ML/TF risks of VASPs that are being registered, including from their client base, products and services provided and geography of operations, as well as quality of their AML/CFT systems and controls. Recommended strengthening of the VASPs sector entry controls appears to require changes to the AML/CFT law to support expanded function of the VASP supervisor and collection of relevant information during VASP registration. The authorities are currently working on amendments with a view to introduce new and strengthen existing AML/CFT requirements for VASPs, such as capital increase, reinforcement of requirements for management staff, linking activities with Lithuania, prohibition of opening anonymous accounts, provisions on "travel rule,"[30] bringing the scope of the VASP definition in

[30] Obligation to obtain, hold, and transmit required originator and beneficiary information, immediately and securely, when conducting VA transfers.

line with the FATF Standards, requiring customer due diligence for all transfers without monetary threshold.[31]

30. In April 2021 a Supervision unit was established in the Lithuanian FIU with responsibility for supervision of obliged entities, including VASPs. The Supervision unit was fully staffed and operational by July 2021, currently consisting of eight staff. Being part of a law enforcement body, the Supervision unit has a strong investigative and law enforcement background and plans to diversify skillset by hiring several non-law enforcement officers with background in data analytics, risk and AML/CFT. In addition, the Lithuanian FIU employs IT tools for data and blockchain analysis and the Analysis division provides analytical support to VASP supervisors. The Lithuanian FIU updated its Selection for Inspection order to introduce elements of a risk-based approach and the Supervision unit commenced on-site inspections of VASPs this year. The identification of VASPs for inspections was based on the suspicious transaction reports to the FIU, public information, with 6 planned inspections for 2022. Completion of the ongoing VASP sectoral analysis, development of offsite monitoring, continuing strengthening supervisory policies and procedures and other supervisory tools is required to develop fully risk-based approach to VASP supervision.

31. The Supervision unit appropriately started its work with developing ML/TF understanding of VA/VASPs, including of the individual Lithuanian VASPs. In 2022, the FIU launched a sectoral strategic ML/TF risk analysis (SRA) of VASPs with the objectives to identify VASPs that provide custodial and VA exchange services, develop understanding of Lithuanian VASPs' client base, including of higher risk clients, types, and value of VASP activities, assessing the quality of VASPs' AML/CFT systems and controls. Conclusions of the sectoral strategic analysis in area of VASP are due in June 2022 and the inspections of VASPs will be carried out later in 2022. To inform the sectoral assessment, the MLPD launched a data collection survey to gather statistics on VASP's number of clients, turnover, profit, and value of client transactions. The SRA also incorporates data from the State Tax Inspectorate on VASPs income declarations, number of registered employees as well as public information (website, advertisements, customer reviews). The SRA can be usefully expanded to analyse the types of VAs with which Lithuanian VASPs are working, as VA vulnerabilities vary significantly depending on the VA design. In addition, countries of VASPs operations can provide useful information regarding VASP's ML/TF risk profile. The SRA should explore what banking and payments arrangements VASPs are using for fiat operations, particularly for conversion of VA to fiat and vice-versa, which is important to understand the degree of exposure of Lithuanian financial sector to risks emanating from VASPs' activities. The authorities should build on the results of the SRA to develop institutional risk assessment methodology with a focus on ML/TF risks of VASP activity, its customer base, type of VA used and quality of AML/CFT controls. Considering current light registration regime under which a significant number of new VASPs have entered Lithuania and improving understanding of ML/TF risks from individual VASPs, the Lithuanian FIU should be granted powers to cancel registration of VASPs with fundamental deficiencies in AML/CFT controls or that face unacceptably high level of ML/TF risk.

Recommendations:

[31] The Parliament has adopted the amendments to the law on the Prevention of Money Laundering and Terrorist Financing strengthening the AML/CFT requirements for VASPs on June 30, 2022.

- Strengthen VASPs market entry controls with a strong emphasis on fitness and propriety tests
- Develop institutional risk assessment methodology and tools for offsite monitoring with a focus on ML/TF risks of VASP activity and VA type based on the sectoral risk assessment results
- Grant the supervisor powers to revoke VASP registration and bring the AML/CFT framework in full compliance with the FATF Standards as related to VA and VASPs.

F. AML/CFT Controls for CENTROlink

32. CENTROlink is a retail payment system operated by the BoL, which represents another emerging area of ML/TF risk. The risk profiles of CENTROlink customers and cross-border reach of its payments pose elevated ML/TF risk that is not adequately mitigated by BoL's AML/CFT systems and controls.

33. BoL opens accounts and provides access to Euro payment infrastructures to various EEA[32]-licensed payment service providers to conduct SEPA[33] national and cross-border payments. The access is granted via CENTROlink—a retail payment system launched in 2015 and operated by the BoL, which provides access to SEPA to various payment service providers (PSPs), banks, credit unions, EMI and PI licensed in the EEA. After connecting to CENTROlink, they may receive access to full range of SEPA services: instant payments, credit transfers, and direct debit services. The BoL also facilitates reception of SWIFT Business Identifier Code and IBAN account numbers for the PSPs and its clients.

34. CENTROlink played an important role in establishment of the Lithuanian fintech hub, providing easier access for EMI and PI to SEPA payments. Access to SEPA payments via CENTROlink was promoted as one of the advantages to conduct business in Lithuania and is a component of the fintech hub's Newcomer Programme facilitating entry of fintechs to Lithuania. CENTROlink is part of the BoL strategic direction towards fostering innovation in the financial sector and development of a FinTech-conducive regulatory and supervisory ecosystem. One of the CENTROlink's objectives is also to promote competition in the financial sector through pricing of access and transaction fees that is lower/competitive with the same services provided by the commercial banks. As Lithuanian banking sector is concentrated and foreign-owned, CENTROlink can also be seen as providing some payment infrastructure redundancy.[34]

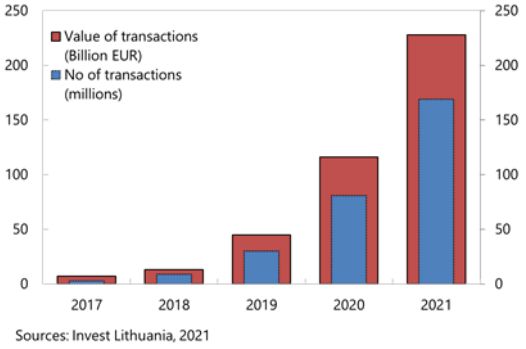
[32] European Economic Area

[33] Single Euro Payments Area

[34] Redundancy defined as duplication of critical functions of a system with the intention of increasing reliability

35. The number of PSPs with access to CENTROlink and the volume and value of transactions conducted via CENTROlink has grown significantly since 2018. Currently, 153 PSPs from 18 EEA countries use CENTROlink services, a significant increase from 90 in mid-2019, which in its turn represented more than doubling from early 2018.[35] Relocation of EMIs from the UK to Lithuania as a result of Brexit is perceived to be one of the main driving forces of this increase. In addition, the U.K.-licensed PSPs account for the highest number of PSPs-customers of CENTROlink after Lithuanian-licensed PSPs. Most of the FIs with access to CENTROlink are EMIs and PIs—131 out of 153, with 86 licensed in Lithuania and 67 in other EEA countries. In 2021, a total of 186 million SEPA payments worth EUR 358 billion were made through the CENTROlink system—a doubling from 95 million payments worth EUR 170 billion in 2020. Most of the payments on CENTROlink are conducted by EMI and PI[36] (Figure 6) for payments not linked to Lithuania. As a result, currently CENTROlink's payments turnover is substantially higher than the inflows to and outflows from Lithuania combined.

Figure 5. E-Money and Payment Institutions Transactions Through CENTROlink



36. The BoL introduced and gradually strengthened AML/CFT controls in granting access to CENTROlink. The BoL introduced an "Enhanced due diligence questionnaire" in early 2021 that is completed as part of PSP onboarding as well as for existing CENTROlink customers. The due diligence questionnaire is broadly based on the Wolfsberg's Group[37] Correspondent Banking Due Diligence Questionnaire, a standard approach to cross-border and other higher risk correspondent banking relationships. While some AML/CFT-relevant information was already collected since 2019, the updated CENTROlink due diligence questionnaire includes 62 questions to PSPs on their AML/CFT staffing, CDD, transaction monitoring, audit, and governance as well as collection of statistics on PSP's customer base and information on PSP business model, enterprise risk assessment, and customer risk rating methodology.

37. The BoL's due diligence questionnaire provides a good basis for ML/TF risk assessment of CENTROlink clients that can be further fine-tuned to reflect Lithuania-specific ML/TF risks. Jurisdictions and licensing authorities of the PSPs that are CENTROlink clients (and any other licensed entity in case of a group) should be directly added to the questionnaire, as it is crucial information for ML/TF risk assessment considering that around half of PSPs CENTROlink clients are not licensed in Lithuania. While the questionnaire gathers data on jurisdictions of incorporation and residency of clients of PSPs, it should be expanded to also cover the jurisdictions of origination and destination of

[35] https://www.lb.lt/en/news/vasiliauskas-lithuania-s-experience-helps-shape-international-fintech-best-practices

[36] The main banks operating in Lithuania execute SEPA regular and instant credit transfers via the pan-European payment systems STEP2-T and RT1 without using CENTROlink.

[37] The Wolfsberg Group is an association of 13 global banks which aims to develop frameworks and guidance for the management of financial crime risks.

payments that the PSP conducts. As the BoL asks in the questionnaire for detailed description of PSP's current business model, it can specify this requirement to provide information on all products and services offered. Cash transactions as a service and cash reporting as part of PSP's AML/CFT program can be also added—as almost all operations of fintech companies are expected to be conducted digitally, any cash transactions can provide useful ML/TF indicators. Scrutiny of possible reliance on third parties to carry out any components of its AML/CFT program can be also added, particularly as new PSP may outsource implementation of AML/CFT requirements. The BoL analyzes various relevant policies and procedures and based on the BoL's understanding of ML/TF risks from foreign PSPs, it can consider adding questions on additional PSP's policies and procedures such as to prohibit the opening of anonymous accounts and accounts for unlicensed FIs.

38. The BoL administers CENTROlink on the basis that it is not covered by AML/CFT requirements. The BoL considers that it doesn't fall under the AML/CFT Standards in operating CENTROlink, as it is not a reporting entity and operating payment infrastructures is outside of the AML/CFT requirements—the existing AML/CFT efforts are seen as additional measures to minimize risks. However, by opening the accounts for PSPs to conduct SEPA transfers, the BoL, in effect, seem to provide cross-border correspondent banking services,[38] a higher risk service according to the FATF Standards. The BoL doesn't consider this as a higher risk service, referring to SEPA regulations as well as FATF Standards[39] that treat all SEPA payments as domestic. However, from the AML/CFT standpoint, payments across national borders and outside of reach of single law enforcement, financial intelligence, and supervisory body still pose elevated ML/TF risk.[40]

39. The customer base, geography of activity, and business model of some CENTROlink customers pose elevated ML/TF risk. Some of the PSPs have business models aimed at high ML/TF risk customers that have difficulties in establishing and maintaining banking relationships, such as VASPs, gambling, and other higher risk sectors. For many of the PSPs CENTROlink is critical to their business model, with 26 percent of fintechs in Lithuania don't have relationships with

[38] FATF Recommendation 13 imposes requirements on cross-border correspondent banking and other similar relationships. FATF Interpretive Note to this Recommendation elaborates that the similar relationships include, for example, those established for securities transactions or funds transfers, whether for the cross-border financial institution as principal or for its customers.

[39] Please see FATF definition of domestic wire transfers – FATF Interpretive Note to Recommendation 16

[40] According to FATF Guidance on Correspondent Banking, October 2016, FATF Recommendation 13 requires additional measures to be applied to cross-border correspondent banking relationships, in addition to performing the CDD and enhanced due diligence measures in FATF Recommendation 10 for high-risk customers. Such additional measures are appropriate because cross-border correspondent banking relationships are seen to be inherently higher risk than domestic correspondent customer relationships

Box 1. Lithuania: FATF Recommendation on Correspondent Banking

Financial institutions should be required, in relation to cross-border correspondent banking and other similar relationships, in addition to performing normal customer due diligence measures, to:

i. gather sufficient information about a respondent institution to understand fully the nature of the respondent's business and to determine from publicly available information the reputation of the institution and the quality of supervision, including whether it has been subject to a money laundering or terrorist financing investigation or regulatory action;
ii. assess the respondent institution's AML/CFT controls;
iii. obtain approval from senior management before establishing new correspondent relationships;
iv. clearly understand the respective responsibilities of each institution.

commercial banks.[41] In addition, as of end-2021, 68 percent of funds of Lithuanian-licensed PSP clients are held with the Bank of Lithuania, compared to 22 percent a year ago, while 21 percent are investments in liquid assets and 11 percent deposits in EU banks.[42] In addition, higher risk countries, including countries under the FATF's increased monitoring, are among the countries that are main destinations of inflows/outflows via CENTROlink. Adopting a risk tolerance document on a high policy level (e.g., BoL Board) would provide guidance on the operational level regarding what type of PSP services, customers, geography of activity are prohibited or restricted to assist in onboarding and conducting ML/TF risk assessment. The BoL has experience in rejecting applicants for CENTROlink access and offboarding customers for various reasons, including AML/CFT concerns—eight applications were rejected in 2021 and 21 institutions have lost access to the system since 2016. The authorities may wish to consider a comprehensive review of all CENTROlink customers based on the expanded due diligence and coverage of all PSP customers by risk assessment as well as in light of potential risk tolerance guidance.

40. CENTROlink's AML/CFT controls require further strengthening to safeguard financial integrity of the European payment infrastructure and BoL reputation. Leveraging the due diligence and customer base questionnaires, the BoL should formalize its existing risk scoring principles, adopting, as already envisaged, a risk assessment methodology to assist in the decision whether to onboard a customer and a risk scoring tool to assign a risk rating that would allow to calibrate the intensity and nature of monitoring of the business relationship As scrutiny of due diligence questionnaire responses and other AML/CFT controls were introduced recently, some PSP customers hasn't been assessed yet, although accounting for the small share of CENTROlink activity. The BoL should cover all CENTROlink customers with the questionnaire and risk assessments, which is particularly important as many of the applicants were granted access to CENTROlink shortly after receiving a license, with onboarding decision based on evaluation of their business plan but without history of operations, while the current nature of their business may deviate from the initial plan. The BoL currently screens transactions to detect potential evasion of targeted financial sanctions, using an external software provider as well as sample testing the transactions to detect any possible misreporting from the PSP clients, for example, regarding the volume of their activity and customer

[41] The Fintech Landscape in Lithuania 2021–2022

[42] Review of the Activities of Electronic Money and Payment Institutions / Q4 2021

base composition. The BoL should strengthen its ongoing monitoring and scrutinize client's transactions for consistency with the BoL's knowledge of the customers, their business model, target geographies and risk profile.

41. The BoL has also established a dedicated team and procedures to address CENTROlink's ML/TF risks, but the level of staffing and resources is inadequate to the volume of CENTROlink payments and the number of PSP clients. Operations of CENTROlink, including AML/CFT controls, is administered by the BOL's payments department—payments system development division which is responsible for customer interaction and front office support. In addition, the BoL has assigned resources to ML/TF risk assessment function to evaluate applicants for CENTROlink access and oversee existing customers from financial integrity standpoint. So far, it conducted 173 risk assessments—53 during the onboarding stage and 120 for existing PSP customers—with only two staff that joined in 2020, limiting the depth of the assessment and degree of scrutiny that can be applied. This appears to fall significantly short of what effective oversight of providing correspondent services to 151 PSP clients, with annual value of transactions exceeding a third of EUR trillion. Current discussions to add an additional employee doesn't seem to address the resource gap. The BoL also developed procedures for due diligence of existing customer and onboarding of customers, which also requires an approval by a committee consisting of the payments department director, head of payments system development division, head of payments systems division, and two AML/CFT risk employees.

42. The BoL should leverage AML/CFT division's expertise and significantly boost resources dedicated to mitigating ML/TF risks from CENTROlink operations. In particular, the AML/CFT experts can join the payments department committee in deciding on onboarding of new customers, participate in formalization of PSP risk scoring methodology, ongoing monitoring procedures and regularly exchange information. In granting access to CENTROlink, the BoL applies neutrality principle by granting access to all PSPs that meet the established criteria from any EEA country and on equal terms. However, quality of supervision is one of the key and most common ML/TF risk factors in assessing an FI—considering that around half of CENTROlink customers are licensed outside of Lithuania - the BoL should nuance its approach to take into account the different quality of AML/CFT supervision of PSPs across EEA countries. Moreover, exchange of information between the BoL and foreign supervisors should be further developed, for example, BoL can benefit from requesting information regarding the level of compliance of PSPs seeking access to CENTROlink. Such exchange of information would be challenging under the current institutional arrangement, as foreign supervisors might not be in a position to share supervisory information with a payments department, underscoring the need to integrate AML/CFT division in CENTROlink oversight.

Recommendations:

- Integrate BoL's AML/CFT experts in CENTROlink onboarding and ongoing monitoring processes and boost the AML/CFT-dedicated resources

- Formalize risk rating methodology to inform CENTROlink onboarding decisions and to assign a risk rating that would allow to calibrate the intensity and nature of monitoring of the business relationship determine intensity of ongoing due diligence
- Strengthen ongoing monitoring of PSP activity in CENTROlink and fine-tune BoL's due diligence questionnaire to reflect Lithuania-specific ML/TF risks