FINANCIAL CRIME
INVESTIGATION SERVICE

MONEY LAUNDERING PREVENTION BOARD

ACTIVITY RESULTS FOR

2025

https://fntt.lrv.lt

TABLE OF CONTENTS

The geopolitical environment in recent years has further underscored the importance of the prevention of money laundering and terrorist financing. The growing risk of the circumvention of sanctions, increasingly complex financial schemes and rapid technological advancements mean that the preventive system must not only function effectively but also be able to anticipate related risks in advance. Today, financial intelligence is an integral part of national security and its effectiveness depends on the ability to identify threats and prevent them in time, and cooperate closely with national and international partners.

Edmundas Jankūnas,
Head of the Money Laundering Prevention Board of the FCIS

To achieve this goal, the resources of the Money Laundering Prevention Board (the Lithuanian Financial Intelligence Unit, hereinafter – the Lithuanian FIU) were consistently strengthened in 2025: the number of employees increased and investments were made in developing their competencies. Considerable attention was also paid to making proposals for the modernisation of the information systems in use, which is planned for the near future.

The enforcement of financial sanctions remained one of the top priorities. Much attention was devoted to the identification of violations and the application of enforcement measures.

The Anti-Money Laundering Authority (AMLA), which began operating at the European Union (hereinafter – the EU) level, has already started implementing the changes to strengthening the anti-money laundering and counter-terrorist financing system, as well as cooperation among the FIUs of EU Member States. The FIU of Lithuania has actively participated not only in various working groups within the FIU composition of the AMLA General Board but also in the supervisory composition of the AMLA General Board, as far as the non-financial sector is concerned. This is important not only for adapting to changes but also for contributing to the development of common standards in this area.

Significant changes have also taken place in the area of supervision of crypto-asset service providers. Until now, this sector was supervised by the Financial Crime Investigation Service, but as of 1 January 2026, the model of supervision has fundamentally changed – only the entities licensed by the Bank of Lithuania may carry out such activities. In preparation for these changes, focused efforts were made to strengthen the cooperation with the Bank of Lithuania not only by aligning the model of supervision but also by conducting joint inspections of virtual currency operators under the inter-institutional cooperation agreement. This has ensured a more consistent and risk-based supervision, more effective identification of potential risks of abuse, and allowed for proper preparation for the changes.

This report presents the statistics and key highlights on the prevention of money laundering and terrorist financing in 2025.

Julita Jagla,
Head of the Compliance Division,
Money Laundering Prevention Board of the FCIS

The year 2025 was significant in strengthening the anti-money laundering and counter-terrorist financing system of Lithuania. The new anti-money laundering framework developed by AMLA in the European Union and the upcoming MONEYVAL evaluation has further highlighted the importance of anti-money laundering and counter-terrorist financing compliance. In this context, we placed much emphasis not only on the regulatory changes but also on their implementation in practice.

The past year has shown that compliance cannot be understood merely as formal adherence to legislation. The new EU requirements, strengthening cooperation and rising expectations indicate that it is not only control that matters, but also the ability to effectively manage risks. Therefore, we have focused more on legislation, supervisory consistency, methodological assistance, and clearer application of requirements in the activities of obligated entities.

The upcoming MONEYVAL evaluation and participation in the development of the new European anti-money laundering framework have further underscored the importance of international cooperation. At the same time, this means that decisions made at the national level must not only be established but must also operate effectively in practice.

I am convinced that only the consistent engagement of institutions, the financial sector and other obligated entities will ensure that compliance in Lithuania is not merely a formality but a practice that works in reality, thus strengthening the transparency and resilience of the entire financial system.

Paulius Stagniūnas,
Head of the Supervision Division,
Money Laundering Prevention Board of the FCIS

Understand. Assess. Monitor.

These are the principles that consistently underpin supervision activities. The sectoral analyses carried out and the conclusions made by the Supervision Division make it possible not only to identify the largest and most relevant operational risks of obliged entities but also to systematically assess them and apply risk-based supervision focused on the highest-risk areas and entities.

This ensures that supervisory actions are targeted, data-driven, and aimed at mitigating specific risks. However, the efforts of the Service or other supervisory authorities alone are not sufficient – the consistent and active involvement of obliged entities is necessary. Effective risk management is only possible when obliged entities actively engage, take responsibility, and apply high standards in their activities.

Marius Staniulis,
Head of the Analysis Division,
Money Laundering Prevention
Board of the FCIS

In 2025, the Lithuanian FIU received 102,763 reports on suspicious monetary operations or transactions (STRs) through the Anti-Money Laundering Information System from financial institutions, other obliged entities, and foreign FIUs. This is the highest number of STRs recorded during the entire monitoring period, reflecting both the increased intensity of financial transactions and the strengthening risk identification practice by obliged entities.

In recent years, the activities of local and international financial and fintech companies have been actively developing in Lithuania, leading to a significant increase in financial flows and greater complexity. These trends are directly reflected in the growth of STRs.

Considerable changes have also taken place in the field of analytical activities. Over the past five years, the Money Laundering Prevention Board has consistently reorganised the analysis processes of STRs and transitioned from the capacity to carry out several hundred analyses per year to systemic solutions enabling the analysis of tens of thousands of STRs.

With the increase in the volume and analytical complexity of STR reports, traditional methods are becoming inadequate for the immediate and comprehensive processing of data. Therefore, the integration of AI solutions into analytical processes is becoming not only a direction for technological progress but also a practical necessity in order to effectively identify and prioritise risks, as well as respond promptly.

01

MONEY LAUNDERING PREVENTION BOARD: ACTIVITY REPORT FOR 2025

In 2025, the activities of the Money Laundering Prevention Board (hereinafter – the MLPB or the Board) of the Financial Crime Investigation Service (hereinafter – FCIS or the Service) under the Ministry of the Interior of the Republic of Lithuania were focused on the performance of financial intelligence functions, the supervision of obliged entities, international and national cooperation, the implementation of international financial sanctions, participation in legislative processes, and preparation for forthcoming European Union and international requirements. The most significant impact on the MLPB's activities stemmed from the increased volume of reports on suspicious monetary operations or transactions (hereinafter – suspicious transaction reports, hereinafter – STRs), the expanding scope of sanctions implementation tasks, preparation for the evaluation by the Committee of Experts on the Evaluation of Anti-Money Laundering Measures and the Financing of Terrorism (MONEYVAL), and active engagement in the development of the framework of the Anti-Money Laundering Authority (hereinafter – AMLA).

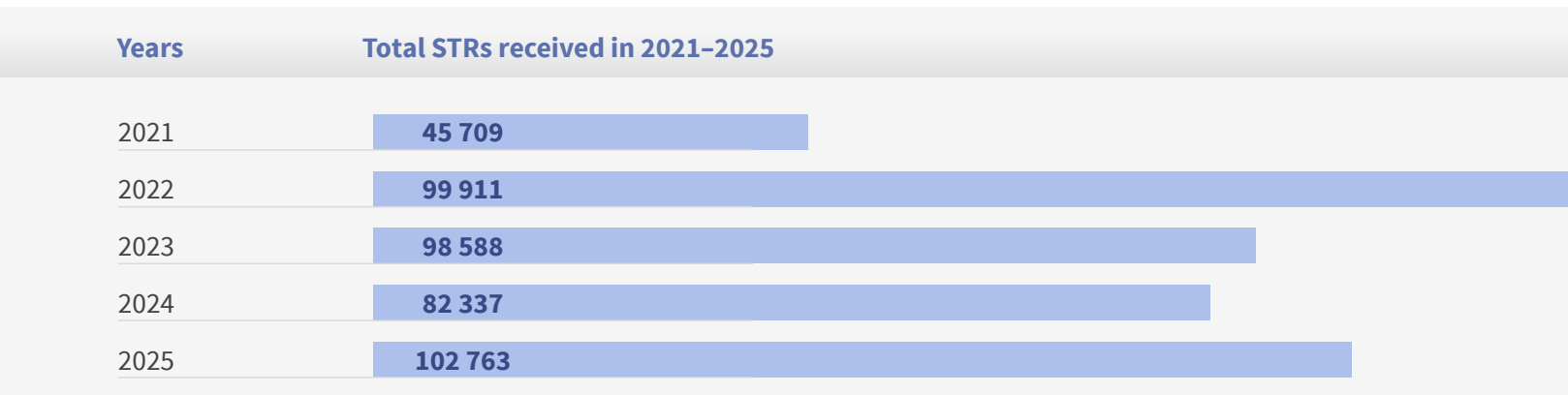
The activities of the MLPB are focused on the performance of financial intelligence functions

REPORTS ON SUSPICIOUS MONETARY OPERATIONS OR TRANSACTIONS

Pursuant to Article 16 of the Law on the Prevention of Money Laundering and Terrorist Financing of the Republic of Lithuania (hereinafter – the LPMLTF), financial institutions and other obliged entities are required to submit STRs to the Service where there are grounds for suspicion of money laundering, predicate offences, or terrorist financing. The Service also receives reports from foreign financial intelligence units (FIUs) where there are reasonable grounds to suspect such criminal activities.

During 2025, 102,763 reports of suspicious monetary operations or transactions were received.

In 2025, the Service's MLPB received a total of 102,763 reports from financial institutions, other obliged entities, and foreign FIUs (2024: 82,337). As illustrated in the chart below, the number of STRs, including those submitted by foreign FIUs, showed a significant increase again compared to previous year. This increase reflects both the strengthening of compliance frameworks among obliged entities and heightened vigilance in identifying potentially illicit financial activity, in line with national and European Union legal standards.



NUMBER OF STR REPORTS RECEIVED IN 2025 BY SECTOR

The table below summarises the STRs received in 2025 by sector, with a comparison to the data for 2024. The data enable an assessment of both the dynamics in the number of reports and their distribution across different categories of obliged entities.

YEAR	2024	2025
Total STRs received, of which:	**82 337**	**102 763**
Foreign Financial Intelligence Units (FIUs)	122	181
FINANCIAL SECTOR, TOTAL:	**73 070**	**88 949**
Banks	69 568	81 578
Specialised banks	143	226
Credit unions	45	65
Currency exchange operators	6	6
Financial brokerage and management companies, life insurance companies, leasing companies	8	6
Money transfer companies	1	0
Payment institutions and electronic money institutions	2 710	6 170
Virtual currency operators, total:	**8 390**	**13 023**
Other obliged entities, total:	**559**	**502**
Notaries	15	21
Bailiffs	2	4
Companies organising gambling and lotteries	541	466
Accountants (persons providing financial accounting or tax advisory services)	0	10
Auditors	1	1
Other (Bank of Lithuania, law enforcement authorities, etc.)	**196**	**108**

As can be observed, the largest number of STRs in 2025 was received from banks and their branches – 81,578 (2024: 69,568). This marked increase in the volume of STRs submitted by banks and their branches may be attributed to the number of fraud cases identified within financial institutions, where reports are submitted not only in relation to accounts used for fraudulent purposes but also in respect of victims of fraud. Furthermore, the growth is significantly driven by technological advancements in the financial sector, including the continuous enhancement of risk monitoring systems, the increasing deployment of automated transaction monitoring, and the application of artificial intelligence solutions, which enable more effective identification of suspicious transaction patterns and potential indicators of money laundering or fraud.

The largest number of STR reports were received by banks, VASP sector companies, and electronic money and payment institutions.

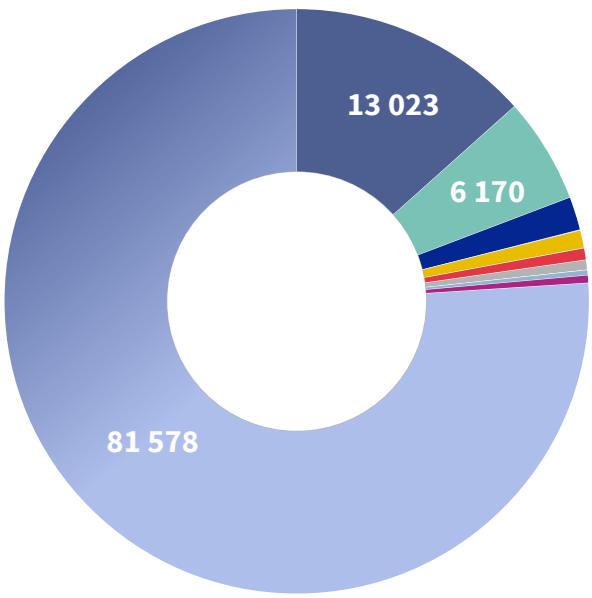
It should be noted that the number of reports received in 2025 from custodial virtual currency wallet operators and virtual asset service providers (hereinafter – VASPs) increased significantly, amounting to 13,023, compared to 8,390 in 2024. The application, as of 30 December 2024, of Regulation (EU) 2023/1114 of the European Parliament and

of the Council of 31 May 2023 on markets in crypto-assets, amending Regulations (EU) No 1093/2010 and (EU) No 1095/2010 and Directives 2013/36/EU and (EU) 2019/1937, as well as the entry into force in Lithuania of the Law on Markets in Crypto-assets adopted on 11 July 2024, have increased compliance and accountability requirements for market participants. It should also be noted that a proportion of market participants, having assessed the forthcoming regulatory requirements in advance and not intending to seek authorisation, may have decided to cease their VASP activities and, prior to discontinuation, submitted accumulated STRs. In addition, the increase in the number of reports may have been further influenced by the licensing process for crypto-asset service providers initiated by the Bank of Lithuania.

A total of 13,023 STRs were received from the VASP sector, of which 5,924 were referred to analysts of the Analysis Division for more detailed examination. By comparison, in 2024, 8,390 such reports were received, of which 2,355 were subject to further assessment. The remaining STRs, following the application of a risk assessment algorithm, were classified as low risk and processed through automated procedures.

In 2025, electronic money institutions and payment institutions submitted 6,170 STRs, ranking as the third-largest sector by volume. The contribution of other groups of obliged entities was significantly lower: money transfer companies submitted 898 reports, gambling operators – 466, specialised banks – 226, foreign FIUs – 181, other obliged entities – 134, and other financial institutions – 87.

The chart below provides an overview of the sectors that generated the highest number of STRs in 2025.



- Banks **81 578**
- Virtual currency operators **13 023**
- Payment/electronic money institutions **6 170**
- Money transfer companies **898**
- Companies organising gambling and lotteries **466**
- Specialised banks **226**
- Foreign FIUs **181**
- Other obliged entities **134**
- Other financial institutions **87**

AUTOMATED ANALYSIS OF REPORTS AND REPORTS ASSIGNED TO ANALYSTS BY SECTOR

Of all reports received in 2025 (102,763), as many as 79,668 were assessed as low risk following the application of a risk assessment algorithm and were consequently finalised through automated processing. By comparison, in 2024, out of 82,337 reports received, 70,920 were similarly classified as low risk and finalised through automated processing.

Accordingly, in 2025, 21,295 reports were assigned to analysts of the Analysis Division for more detailed examination (2024: 10,026).

The statistics below present the distribution, by sector, of STRs assigned to analysts of the Analysis Division for in-depth analysis in 2024–2025.

In 2025, 21,295 reports were assigned to analysts from the Analysis Division for more detailed analysis (2024 – 10,026).

SECTOR	2024	2025
Total:	**10 026**	**21 295**
Foreign Financial Intelligence Units (FIUs)	122	181
FINANCIAL SECTOR:	**6 996**	**14 644**
Banks	4 518	10 116
Specialised banks	128	224
Credit unions	42	65
Currency exchange operators	3	6
Financial brokerage and management companies, life insurance companies, leasing companies	6	3
Money transfer companies	1	0
Payment institutions and electronic money institutions	1 865	3 640
Virtual currency operators	**2 355**	**5 924**
Other obliged entities:	**553**	**546**
Notaries	15	19
Bailiffs	2	4
Gambling and lottery operators	533	463
Accountants (persons providing financial accounting or tax advisory services)	0	6
Auditors	1	1
Other (Bank of Lithuania, law enforcement authorities, etc.)	**241**	**53**

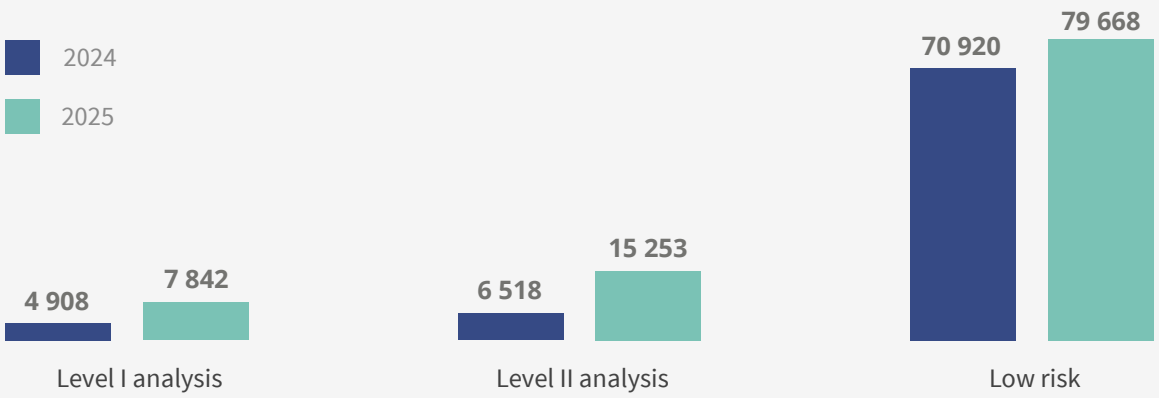
As evidenced by the statistical data for 2024–2025, the most significant increase was recorded in the financial sector, where the number of STRs assigned to analysts rose from 6,996 to 14,644. The largest growth was observed in reports submitted by banks and their branches: in 2025, 10,116 such reports were assigned for analysis, compared to 4,518 in 2024.

A significant increase was also recorded in the payment and electronic money institutions sector, where the number of reports assigned for analysis rose from 1,865 to 3,640. Moreover, following the increase in reports received

from virtual currency operators, the number of reports from this sector assigned for analysis more than doubled – from 2,355 in 2024 to 5,924 in 2025. This trend indicates that, in 2025, the principal analytical workload was concentrated in the banking sector, as well as in the payment and electronic money institutions sector and among virtual currency operators.

Meanwhile, in the group of other obliged entities, the number of reports assigned to analysts remained broadly stable at 547, compared to 554 in 2024. In the sector of gambling and lottery operators, a slight decrease was recorded, from 533 to 463 reports. The number of reports assigned for analysis from other reporting entities, including the Bank of Lithuania, law enforcement authorities and other bodies, declined from 241 to 53.

The chart below presents the distribution of STRs in 2024–2025 according to risk level, distinguishing between low-risk reports and those subjected to Level I and Level II analysis.



As shown in the chart, in both 2024 and 2025, the largest proportion of STRs was classified as low risk, amounting to 70,920 reports in 2024 and 79,668 in 2025. At the same time, in 2025, the number of reports requiring more detailed assessment increased significantly. STRs assigned for Level I analysis rose from 4,908 in 2024 to 7,842 in 2025, while those assigned for Level II analysis increased from 6,518 to 15,253. This indicates that, despite the continued predominance of low-risk reports, the volume of more complex cases requiring additional scrutiny grew substantially in 2025.

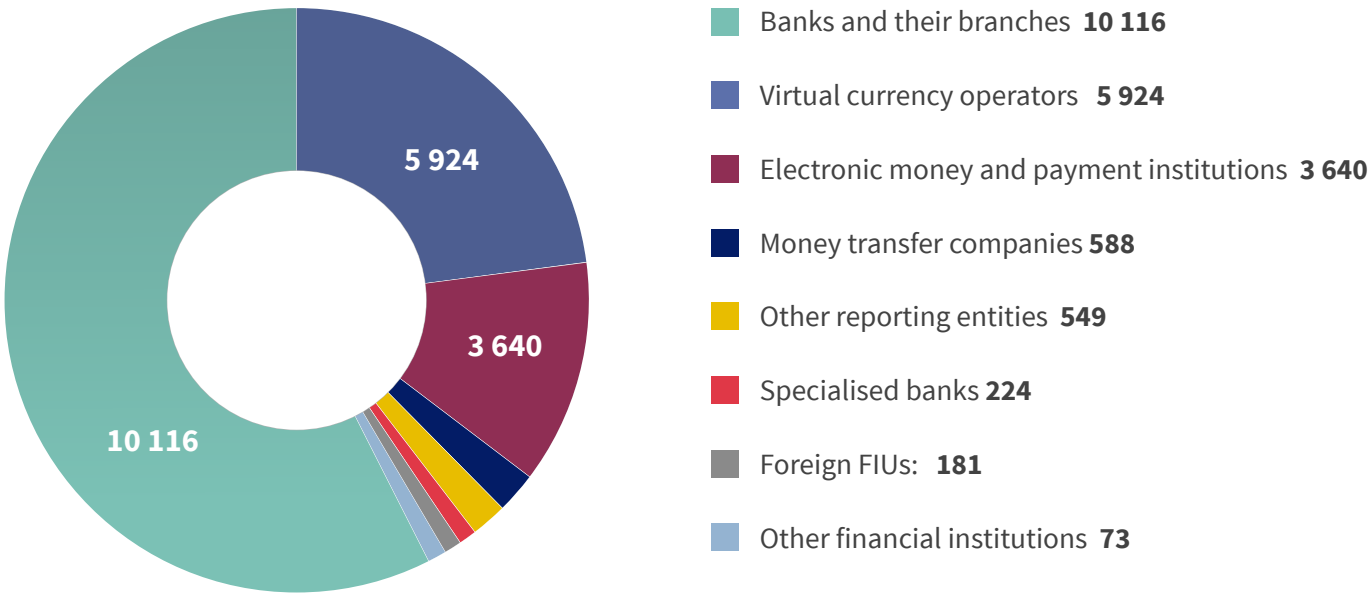
Pursuant to Clause 13.2 of the Money Laundering Prevention Board's analysis procedure, approved by Financial Crime Investigation Service Director's Order No. V-92 of 18 May 2017, reports assigned for Level II analysis require only the preparation of a conclusion regarding the conducted analysis. In contrast, Level I analysis reports demand a more detailed assessment, for which official service reports are drafted, describing the course of the analysis. In light of this, it can be stated that in 2025 the analytical workload of the MLPB not only increased quantitatively but also became more intensive in terms of content and scope of evaluation.

In 2025 the flow of STRs not only increased but also involved a greater scope of analytical assessment.

It should also be noted that in 2025 the number of reports received from foreign financial intelligence units and assigned for analysis increased to 181, compared to 122 in 2024. The information received most frequently concerned potential money laundering cases, followed by reports related to fraud, and, in third place, possible breaches of international sanctions. This demonstrates that the importance of international information exchange remains high, and the data received encompass a broad spectrum of risks.

In summary, it can be concluded that in 2025 the flow of STRs not only increased but also involved a greater scope of analytical assessment. Although the majority of reports continued to be classified as low risk, the significant rise in reports assigned for Level I and, in particular, Level II analysis indicates an increased need for additional scrutiny. This suggests that in 2025 the analytical workload of the MLPB's analysts grew both quantitatively and qualitatively, while information received through international cooperation channels remained essential in identifying potential cases of money laundering, fraud, and sanctions violations.

The chart below presents the distribution of STRs assigned for Level I and Level II analysis in 2025, broken down by sector.



As shown in the chart, in 2025 the STRs assigned for Level I and Level II analysis were predominantly submitted by banks and their branches, with a significant proportion also coming from virtual currency operators and the electronic money and payment institutions sectors. This indicates that the main analytical workload in 2025 was concentrated in these sectors.

It was also observed that the number of reports submitted by virtual currency operators and assigned for analysis increased in 2025.

Analysis of reports received in 2025 concerning clients' suspicious financial activity revealed an increase in the number of analyses assigned in certain sectors. Nearly twice as many reports were submitted by specialised banks – 224 (2024: 128) – and money transfer companies – 588 (2024: 433). This growth is attributed to the fact that some financial institutions operating in Lithuania provide services not only to local clients but also to citizens of other countries, resulting in a significantly larger client base and transaction volume. Additionally, financial institutions are investing in advanced transaction monitoring systems, automated risk assessment tools, and compliance functions, enabling more effective detection of suspicious activity patterns, which in turn increases the number of reports submitted.

It should be noted that the number of STRs assigned for analysis from non-financial obliged entities remained low in 2025, although positive trends were observed in certain sectors. The gambling and lottery sector continues to be one of the most active STR submitters in the non-financial sector; however, in 2025 the number of reports received and assigned for analysis decreased to 463 (2024: 533). A positive development was also observed in the activities of providers of financial accounting and tax advisory services. While in 2024 no STRs from this sector were assigned for

analysis, in 2025 there were 6 such reports. This indicates a growing engagement of this sector in the implementation of anti-money laundering requirements.

Despite these positive developments, some non-financial obliged entities – such as real estate agents, lawyers, individuals conducting cash transactions exceeding €10,000 (e.g., vehicles traders), persons engaged in the trade of precious metals or gemstones, operators of movable cultural property and antiques, and providers of trust or company formation and administration services – continued not to submit STRs, even though they are legally required to do so under anti-money laundering and counter-terrorist financing regulations.

In order to effectively implement Recommendation No. 29 of the Financial Action Task Force (FATF), the MLPB has, since 1 September 2021, provided financial institutions and other obliged entities with STR quality assessments using a five-point scale, aiming to improve the quality of submitted reports. This measure is recognised by foreign FIUs as a best practice. In 2025, STRs submitted by banks were rated 4 and 5, indicating that the reports were detailed and clear, the necessary attachments were provided, or the report was used effectively with a thorough and clear description and accompanying documentation. In contrast, reports from VASPs and other entities received ratings of 1, 2, and 3, reflecting issues such as missing attachments, unclear report descriptions, or inaccurate reporting of entity information.

OTHER REPORTS RECEIVED FOR ANALYSIS

In addition to information submitted by obliged entities, the MLPB also receives reports from the Bank of Lithuania's Strategy and Governance Department. These reports provide information on individuals' cash exchange transactions exceeding €15,000, structuring or layering operations, the exchange of damaged banknotes, and other relevant cases. They also include information on entities assessed by the Bank under its established procedures to determine the sources of clients' assets and funds.

In 2025, the MLPB received 48 such reports, the majority of which were assigned for Level II analysis (2024: 233 reports). The MLPB also receives information from other law enforcement agencies, as well as from natural and legal persons in Lithuania and abroad, which serves as a basis for conducting additional analyses of entities' financial activities.

NUMBER OF MATERIALS FORWARDED BASED ON RECEIVED STRS

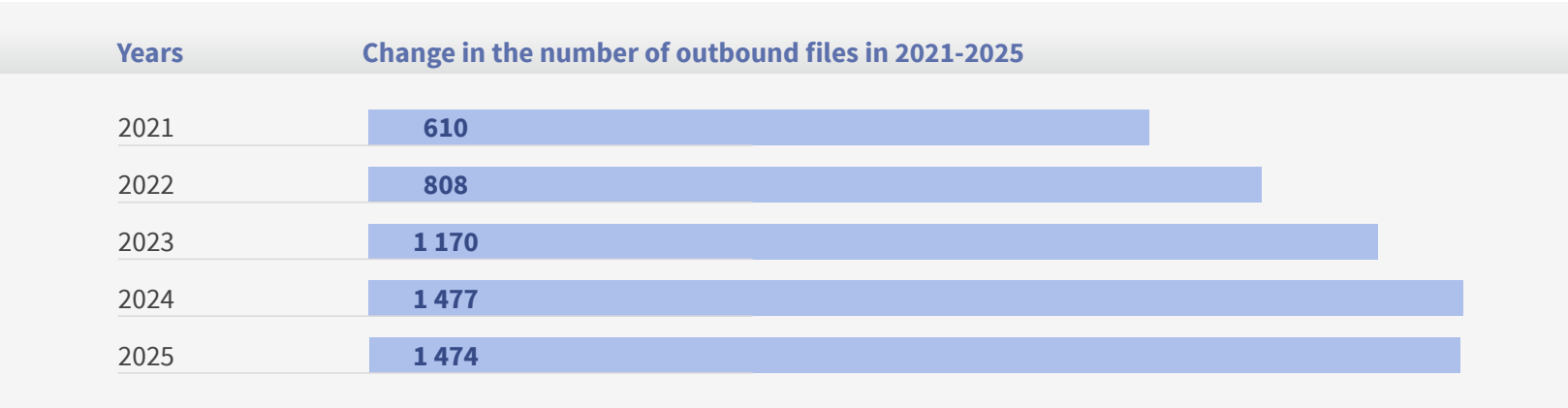
In 2025, following the analysis of received STRs, 1,474 sets of materials regarding entities' suspicious financial activity were forwarded to the Service's divisions, other state and law enforcement institutions, and foreign financial intelligence units for further examination and assessment (2024: 1,477).

In 2025, after the analysis, 1,474 sets of materials were forwarded to the Service's departments and other institutions in Lithuania and abroad for further examination.

	2024	2025
Service's units	50	45
State Tax Inspectorate	63	73
Law enforcement and other state authorities	245	239
Foreign FIUs	1 119	1 117

As shown in the previously presented chart, 357 sets of materials were forwarded to the Service's divisions, Lithuanian law enforcement authorities, and other state institutions for further investigation, examination, or assessment (2024: 358). The majority of these materials were sent to the Lithuanian Police divisions – 177 (2024: 147), reflecting a significant increase primarily related to fraud cases, including investment schemes targeting Lithuanian and foreign citizens via various platforms, unlawful access to account data, and other types of fraud. Materials forwarded to the State Tax Inspectorate under the Ministry of Finance remained at a similar level, with a slight increase from 63 to 73. Meanwhile, the number of materials forwarded to the State Security Department (VSD) of the Republic of Lithuania decreased from 39 to 32, to other law enforcement and state institution divisions from 59 to 30, and to the Service's own units from 50 to 45. Considering the overall distribution of forwarded information, the majority of materials were sent to foreign financial intelligence units – 1,117 reports (2024: 1,119). Additionally, following analysis, 1,596 reports (2024: 784) were transmitted in XBR format (Cross-Border Reporting), indicating that a significant portion of identified suspicious financial activity involves an international element and requires active international cooperation.

It should be noted that some of the STRs received were related to the financial activities of politically exposed persons (PEPs). In 2025, 32 such reports were received (2024: 31), including 5 reports concerning foreign PEPs. This indicates that the number of reports in this category remained stable. Following analysis, the majority of these reports were, according to competence, forwarded to the Special Investigation Service (STT) or to foreign FIU.



As shown in the chart, the number of materials forwarded steadily increased from 2021 to 2024, while in 2025 it remained essentially stable, decreasing only slightly from 1,477 to 1,474. This suggests that the Board's operational volume has remained consistently high.

It should also be noted that in 2025 a total of 4,138 reports were sent to foreign financial intelligence units in XBR format, whereas in 2024, using the automated transmission functionality of FIU.net, 37,210 reports were transmitted. This difference is attributable to the fact that the current version of the FIU.net network does not yet support automated transmission functionality. At the same time, the number of XBR-format reports received from foreign financial intelligence units in 2025 increased to 6,908, compared to 4,114 in 2024.

PRELIMINARY CRIMINAL INVESTIGATIONS INITIATED BASED ON MATERIALS FORWARDED BY THE MLPB

Based on materials forwarded by the MLPB regarding the suspicious financial activities of natural and legal persons, the Service's divisions initiated 5 preliminary criminal investigations in 2025 (2024: 16). Of these, one investigation was initiated under Article 216 of the Penal Code of the Republic of Lithuania ("Laundering of Crime-Related Property") (2024: 4).

Other preliminary criminal investigations were initiated under Articles 184 ("Misappropriation of property"), 202 ("Unauthorised Engagement in Economic, Commercial, Financial or Professional Activities"), 220 ("Provision of Inaccurate Data on Income, Profit or Assets"), and 222 ("Fraudulent Management of Accounts") of the Penal Code of the Republic of Lithuania.

REPORTS ON SUSPENDED FINANCIAL TRANSACTIONS

Years	Total reports on suspended funds (number)	Suspended amounts (EUR millions)
2021	253	65
2022	565	162
2023	484	53,5
2024	530	79
2025	893	71

As shown in the chart, in 2025 the number of reports regarding funds suspended in clients' accounts increased significantly, reaching 893 reports, compared to 530 in 2024. The majority of these reports were related to cases of fraud or to unidentified sources of funds, where clients failed to provide financial institutions with the requested documentation substantiating the origin of the funds.

In 2025, the number of reports received regarding funds suspended in clients' accounts increased to 893 reports.

At the same time, despite the increase in the number of reports, the total amount of suspended funds decreased, amounting to nearly €71 million in 2025, compared to over €79 million in 2024. Of this amount, approximately €2.4 million was subsequently subjected to a temporary restriction of ownership rights in accordance with the procedures established by the Criminal Procedure Code of the Republic of Lithuania (2024: €7.2 million).

The amount of suspended funds in 2025 reached almost 71 million euros.

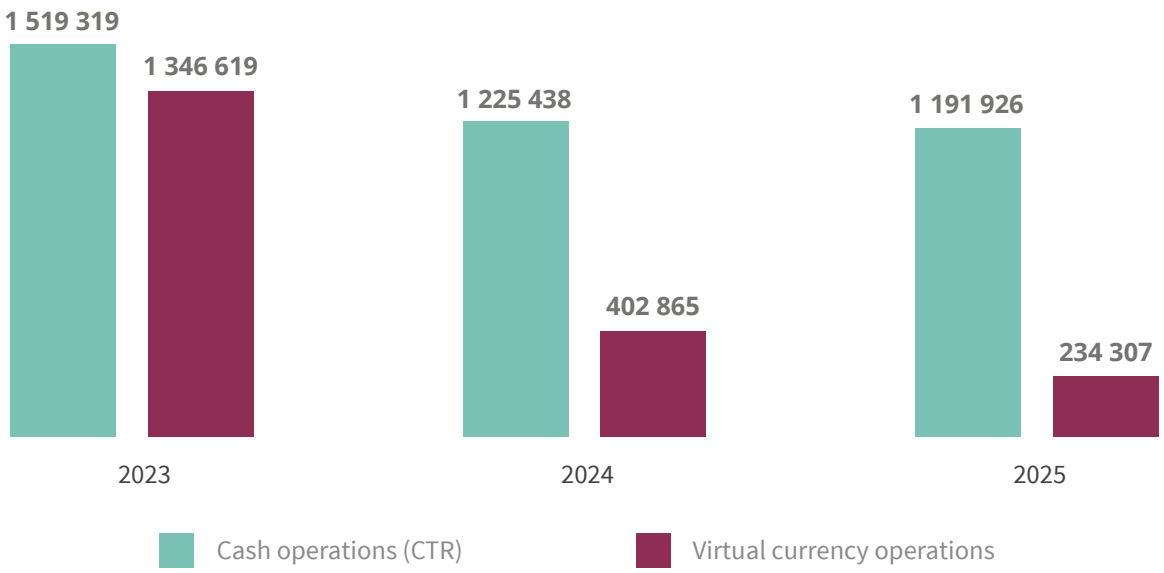
The decrease in the total amount of suspended funds, despite the higher number of reports, may be attributed to obliged entities suspending smaller amounts (sometimes only a few euros) and to consultations and training provided by MLPB specialists. Before submitting STRs concerning suspended funds, responsible personnel at obliged entities increasingly conduct more thorough internal investigations, collect the necessary data, and only then decide whether to file a report. This suggests that the practice of reporting is becoming more consistent and that the information submitted is better substantiated.

Following analysis by the MLPB's analysts, collected information is most often forwarded to police divisions or foreign financial intelligence units for further investigation. In cases where the received information is not

It should be noted that in 2025 the MLPB executed 311 requests to freeze funds—both those received from foreign FIUs concerning accounts in Lithuanian financial institutions and from Lithuanian law enforcement authorities concerning accounts abroad—exceeding the 292 requests processed in 2024.

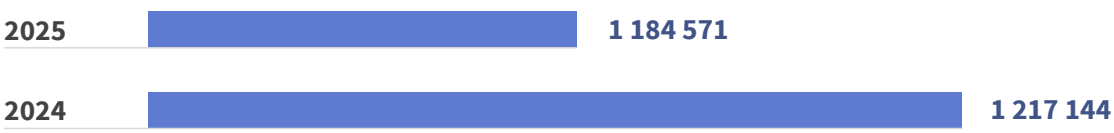
REPORTS ON CASH AND CRYPTO-ASSET TRANSACTIONS

Pursuant to Article 20 of the LPMLTF, obliged entities are required to provide the Financial Crime Investigation Service with information on a client's identity and the transactions conducted when cash or crypto-asset operations reach €15,000 or more. This obligation applies both to cash transactions and to information provided by entities in the virtual currency sector according to procedures established by the Service.

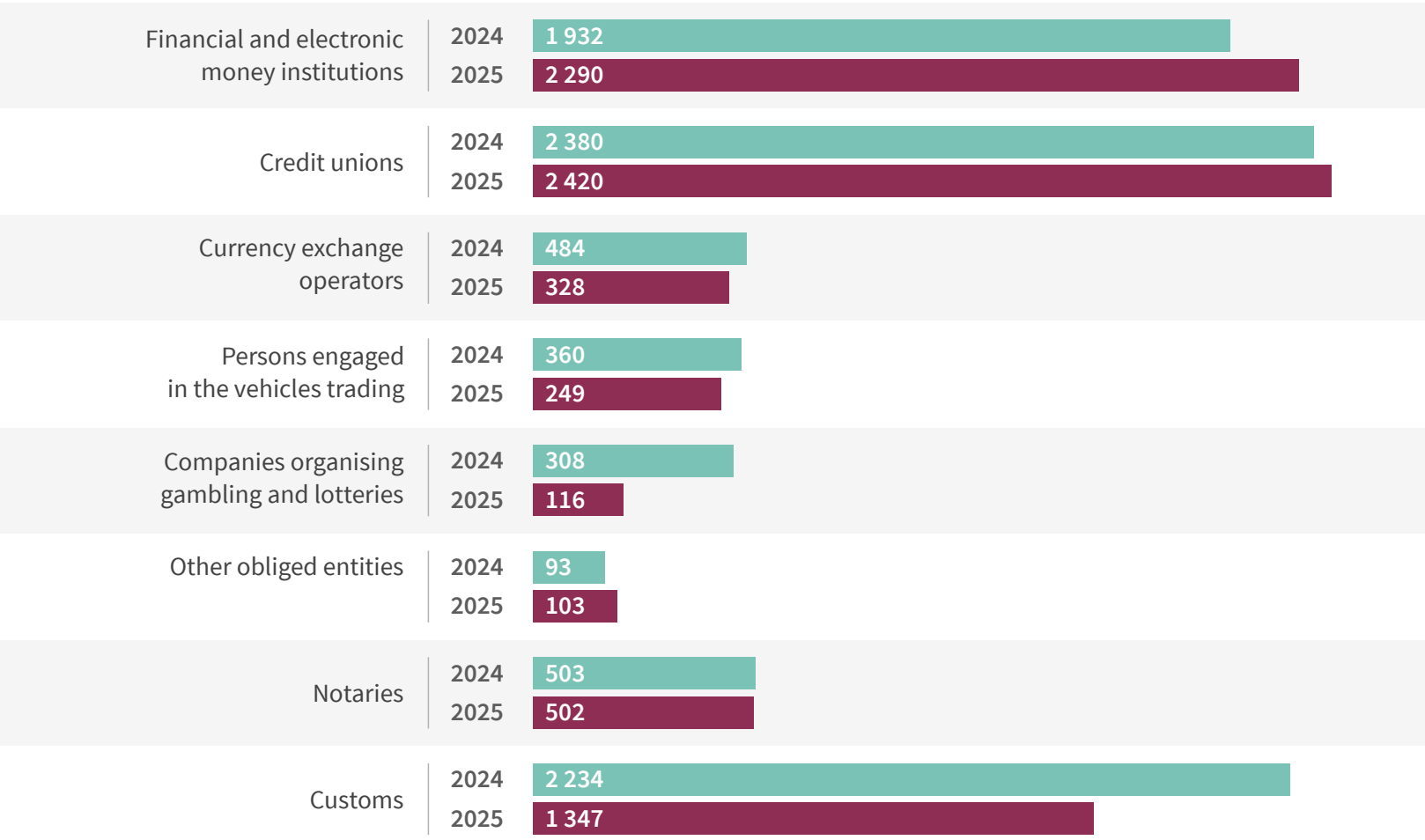


As shown in the chart, the number of reports on cash transactions received between 2023 and 2025 remained consistently high but gradually decreased – from 1,519,319 reports in 2023 to 1,191,926 reports in 2025. The largest share of these reports, covering cash deposits, exchanges, and withdrawals, was submitted by banks:

Banks



Other obliged entities



Meanwhile, the decline in reports on virtual currency operations was much more pronounced: 1,346,619 reports were received in 2023, 402,865 in 2024, and 234,307 in 2025.

02

NATIONAL COOPERATION

REQUESTS FOR INFORMATION

In 2025, the MLPB continued cooperation with the Service's divisions and Lithuania's competent authorities, exchanging financial intelligence information. During the year, the Board received 241 requests for financial intelligence information, other related data, and assistance in freezing funds in foreign financial institutions (2024: 307).

The chart below illustrates the number of institutions submitting information requests to the Service from 2021 to 2025.

INSTITUTIONS	2021	2022	2023	2024	2025
Police units (incl. Lithuanian Criminal Police Bureau)	221	224	154	154	130
State Security Department	5	5	1	1	1
Special Investigation Service	1	0	1	1	0
State Tax Inspectorate	5	2	2	7	1
Bank of Lithuania	349	343	11	10	9
Other institutions	180	288	115	43	28
Service units	83	103	97	91	72
Total	**844**	**965**	**381**	**307**	**241**

In 2025, the MLPB received 134 requests from law enforcement and other state institutions for information or for the freezing of funds in financial institution accounts (2024: 162). Analysis of these requests showed that, as in 2024, they primarily concerned client accounts that may have received funds through fraudulent schemes – both from within Lithuania and from abroad – or involved transfers to foreign financial institution accounts. The requests typically related to identifying account holders and ultimate beneficiaries, tracing subsequent fund movements, and freezing funds in accounts. Additionally, institutions requested that the MLPB contact foreign FIUs for information on account ownership, data on natural and legal persons, existing accounts, fund flows, and fund freezes in foreign financial institutions, as well as provide the Service's financial intelligence and other relevant information for investigations conducted by Lithuanian Police divisions.

In 2025, cooperation with other Service divisions also continued. Through the Document Management General Information System, 72 requests were received (2024: 91), seeking information on entities, including received STRs and reports on cash transactions, suspicious financial activities conducted by the entities, and accounts held in foreign financial institutions. The requests additionally involved assistance in freezing funds in foreign financial institution accounts and the provision of account statements, account opening documents, and other information relevant to ongoing investigations.

In 2025, 9 requests were received from the Bank of Lithuania (2024: 10), relating to information on natural and legal persons under review in Lithuania and abroad, provided during licensing procedures or client funds assessment processes.

As shown in the table, the number of requests for information received from 2021 to 2025 exhibited a declining trend: from 844 requests in 2021 and 965 in 2022, to 381 in 2023, 307 in 2024, and 241 in 2025. This indicates that, following the particularly intensive period of 2021–2022, the flow of requests has stabilised at a lower level.

The largest share of requests in 2025, as in previous years, came from police divisions and the Lithuanian Criminal Police Bureau – 130 out of 241, i.e., more than half of all requests received. This confirms that within the context of national cooperation, the MLPB's most important institutional partners remain in law enforcement, particularly in investigations related to fraud, fund movements, and potential asset concealment.

Meanwhile, the number of requests received from the Service's own divisions decreased from 91 in 2024 to 72 in 2025, and from other institutions – from 43 to 28. The number of requests from the Bank of Lithuania remained almost unchanged compared to 2024, at 9 requests; however, over a longer period, there has been a sharp decline compared to 2021–2022, when there were 349 and 343 requests, respectively. This suggests that both the nature and volume of requests from these institutions have changed significantly in recent years.

In 2025, the number of requests from the State Security Department, the Special Investigation Service and the State Tax Inspectorate remained very low. This indicates that the main flow of national information exchange was primarily concentrated within police divisions, the Service's internal divisions, and, to a limited extent, the activities of the Bank of Lithuania.

The information available to the MLPB was most relevant in investigations conducted by police related to fraud schemes.

In summary, national cooperation in the field of financial intelligence remained active in 2025, even though the total number of requests continued to decline compared to previous years. The greatest demand for the MLPB's information continued to come from police divisions, primarily in investigations related to fraud schemes, tracing fund movements, and freezing assets. This demonstrates that the MLPB's role in national institutional cooperation remains significant, particularly in providing financial intelligence that can be used operationally.

03

INTERNATIONAL COOPERATION

The Money Laundering Prevention Board actively cooperated with foreign financial intelligence units in 2025, exchanging information via the FIU.net and Egmont Secure Web (ESW) networks. That year, the MLPB received 1,586 requests from foreign FIUs, up from 1,422 in 2024.

Information is exchanged via the FIU.net and Egmont Secure Web (ESW) networks. In 2025, 1,586 requests were received. The majority of requests were related to potential money laundering, as well as fraud cases.

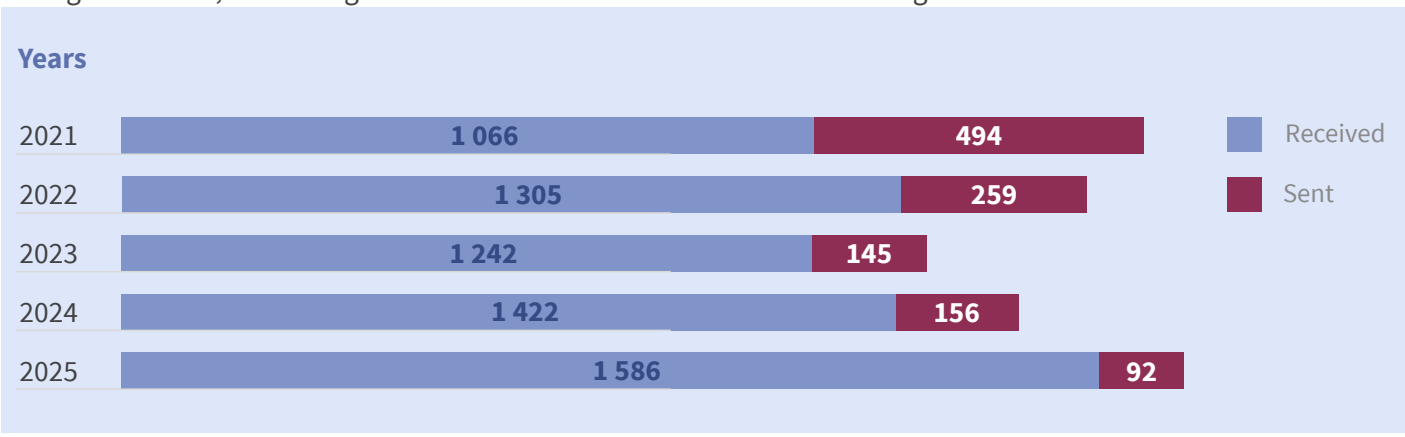
Analysis of the requests showed that the individuals and legal entities under review often used the services of financial institutions and virtual currency service providers registered in Lithuania, holding accounts with these entities. Most requests related to potential money laundering and fraud, including cyber and investment fraud. Requests concerning tax evasion, terrorist financing, breaches of international sanctions, or other criminal activities were less frequent.

Analysis of the requests by the origin of the subjects revealed that the majority involved foreign nationals or foreign companies using the services of Lithuanian financial institutions. Lithuanian citizens or companies were mentioned relatively infrequently and represented only a small proportion of all cases.

A clear trend was observed in which funds, potentially linked to fraudulent activities—such as investments in fictitious platforms – were transferred into accounts held at financial institutions registered in Lithuania. These funds were often subsequently moved to accounts or financial platforms in other countries, suggesting that some accounts opened in Lithuania by foreign entities are being used as transit accounts.

Analysis of requests sent to foreign FIUs shows that in 2025 their number decreased to 92 (2024: 156). These requests sought information regarding Lithuanian natural and legal persons, their accounts at foreign financial institutions, their activities, connections, and other information relevant to ongoing investigations.

The chart below presents the number of requests received from and sent to foreign financial intelligence units during 2021–2025, illustrating the trends in cross-border information exchange.



As shown in the chart, the number of requests received from foreign FIUs steadily increased from 1,066 in 2021 to 1,586 in 2025. Meanwhile, the number of requests sent to foreign FIUs fluctuated and in 2025 amounted to 92 (compared to 156 in 2024). The statistics indicate that international cooperation remains very active and constitutes a significant part of the MLPB's activities.

INBOUND REQUESTS FROM FOREIGN FIUs IN 2025, BY COUNTRY

Analysing the distribution of requests by country, it is evident that the majority of requests in 2025 continued to be received from European Union member states.

The largest number of requests received from Latvia (149), Malta (120), Slovenia (102).

The highest number of requests in 2025 was received from Latvia (149), Malta (120), Slovenia (102), Portugal (96), Germany (88), and Finland (84). A notable number of requests also came from France, Luxembourg, Poland, Sweden, Belgium, and Cyprus. Requests from other countries were fewer, and comparatively few requests were received from third countries.

This indicates that international cooperation is primarily conducted within the European Union, although connections with third countries are also maintained.

Latvia	149	Estonia	34	United States	6
Malta	120	United Kingdom	32	United Arab Emirates	6
Slovenia	102	Netherlands	32	Romania	6
Portugal	96	Norway	28	Switzerland	6
Germany	88	Ukraine	26	Monaco	5
Finland	84	Slovakia	22	Gibraltar	3
France	74	Bulgaria	20	New Zealand	3
Luxembourg	73	Czech Republic	19	San Marino	3
Poland	62	Greece	14	Albania	2
Sweden	57	Croatia	13	Australia	2
Belgium	56	Montenegro	12	Azerbaijan	2
Cyprus	55	Moldova	11	Qatar	2
Italy	48	Ireland	8	Liechtenstein	2
Spain	47	Turkey	8	Isle of Man	2
Hungary	45	Kazakhstan	7	Syria	2
Denmark	37	Bosnia and Herzegovina	6	Uzbekistan	2

OUTBOUND REQUESTS TO FOREIGN FIUs IN 2025, BY COUNTRY

In 2025, a total of 92 requests were sent to foreign financial intelligence units (compared to 156 in 2024). Most requests were directed to Germany and the United Kingdom, as well as Italy, Portugal, Poland, and Belgium.

The largest number of requests were sent to Germany, the United Kingdom, and Italy.

Overall, the distribution shows that requests were sent to a wide range of countries, with most receiving only one or a few requests. This indicates a balanced and evenly distributed pattern of international cooperation.

Germany	10	Canada	2	South Korea	1
United Kingdom	9	Latvia	2	Croatia	1
Italy	6	Netherlands	2	Luxembourg	1
Portugal	6	Romania	2	Malta	1
Poland	5	Singapore	2	Isle of Man	1
Belgium	4	Turkey	2	Nigeria	1
Cyprus	3	Ukraine	2	South Africa	1
Slovakia	3	Brazil	1	France	1
Ireland	2	Denmark	1	Seychelles	1
Bulgaria	2	Gibraltar	1	Sweden	1
Estonia	2	Greece	1	Switzerland	1
Israel	2	Spain	1	Uzbekistan	1
United Arab Emirates	2	Japan	1	Hungary	1
Montenegro	2	Kazakhstan	1		

In 2025, international cooperation remained intensive and continued to grow steadily, with information exchange primarily taking place with European Union Member States. The increasing number of incoming requests indicates active engagement by foreign partners and a significant role of the MLPB in international information exchange. This is also influenced by the fact that financial institutions operating in Lithuania provide services to clients across Europe. This allows the MLPB to be regarded as a reliable and active participant in international financial intelligence cooperation.

RECEIVED REQUESTS UNDER DIRECTIVE (EU) 2019/1153

In 2025, in the context of implementing Directive (EU) 2019/1153 of European Parliament and of the Council (EU), the MLPB received 10 substantiated requests from Europol for financial or financial analysis information under Article 5^1 of the LPMLTF, compared to 4 requests in 2024.

This directive establishes rules for the simplified use of financial and other information for the prevention, detection, and investigation of criminal activities, and its provisions came into force in Lithuania on 1 August 2021.

04

ANALYTICAL OVERVIEW

KEY TYPOLOGIES OF SUSPICIOUS FINANCIAL TRANSACTIONS

Based on the STR reports received in 2025 and the subsequent analyses, the most common and recurring typologies and schemes of suspicious financial transactions have been identified. These typologies reflect the most relevant money laundering, fraud, and other financial crime patterns encountered by financial institutions, other obliged entities, and law enforcement agencies.

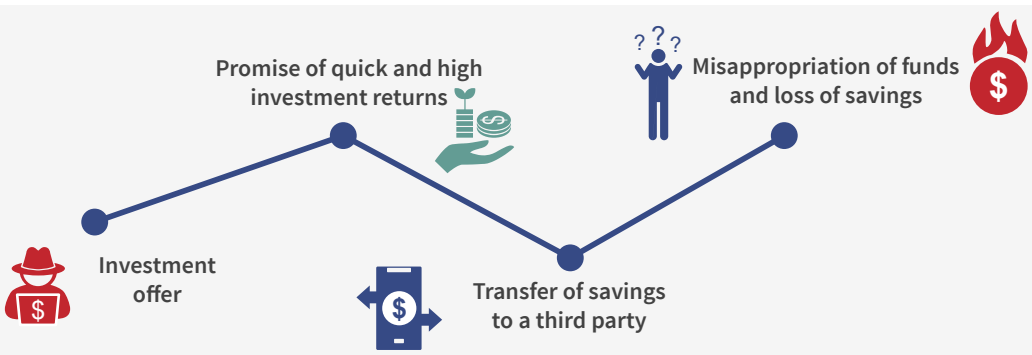
The following are the most significant typologies and schemes identified in 2025.

Based on the STR reports received in 2025, the most common typologies related to money laundering, fraud, and other financial crimes.

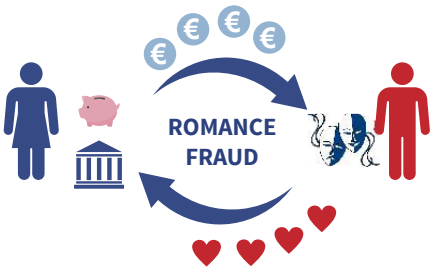
FRAUD

It has been observed that fraud has, for many years, been the most widespread criminal activity in the digital environment and accounts for a large proportion of reports on suspicious financial transactions or operations. The reports feature various forms of fraud – investment or romance scams, email fraud (phishing), telephone fraud, voice call fraud (vishing), SMS fraud (smishing), online shopping fraud, fraud when accessing electronic service providers' websites, and when purchasing goods or tickets for concerts and other events via classified ad platforms or social media, among others.

Investment fraud aims to deceitfully extract money from individuals by promising high returns on investments. Enticed by the idea of easy and quick profits, victims often take out payday loans, borrow from friends, involve family members, and transfer their savings to the fraudsters, hoping for unrealistically high investment returns. Currently, a particularly widespread form of this fraud involves virtual currency investments – fraudsters contact potential victims via telephone, email, or social media, typically targeting individuals with limited knowledge of virtual currencies, and persuade them to transfer their funds so that the person posing as an investment expert can "invest" the money in virtual currency and generate investment returns. Funds are often transferred through multiple bank accounts, sometimes involving foreign entities, so-called money mules, before ultimately being moved to various virtual asset exchanges, thereby making the money trail extremely difficult to trace. In some cases, the fraudsters disappear as soon as they receive the funds; in others, the victim may see the supposed value of their investment grow, but encounters problems as soon as they try to transfer the funds to another platform, account, or to withdraw them. Investment fraud frequently affects middle-aged and older individuals, who may hand over their entire savings and, in some cases, even take out payday loans to invest.



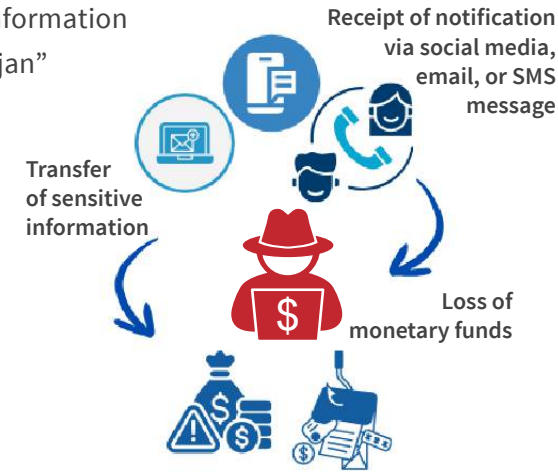
Romance fraud are common on social media and dating platforms – a perpetrator posing as a single individual approaches a potential victim, claiming to want to get to know them, and employs various manipulation techniques, exploiting the victim's emotional attachment. The scammer may ask for money, citing life-threatening situations, or request funds to purchase travel tickets for a supposed meeting, among other tactics. Both men and women fall victim to romance scams – the victim voluntarily gives money to a stranger, often distrusting warnings from family, financial institutions, or even the police about the potential fraud.



There have been cases where elderly individuals were deceived by an organised group of fraudsters. The victim was asked to pay for the treatment of a "friend" – a person claiming to be a soldier who had been injured during war and was receiving medical care abroad. Over a period of time, the victim transferred more than €10,000 to various individuals posing as doctors, assistants, and other persons allegedly caring for the supposed soldier friend.

Phishing, vishing, and smishing are forms of electronic fraud classified as social engineering attacks, aimed at deceitfully obtaining confidential information – such as personal data, login credentials, passwords, and bank card details. Information is typically sought through emails that impersonate trusted organisations or institutions, by phone calls posing as legitimate representatives of banks, police, or other authorities, and via SMS messages containing fraudulent links or requests to verify personal information. This year, there has been a notable increase in fraud cases involving the creation of fake websites – such as "e.sveikata," "VMI," "e.draudimas," "Registrų centras," and "Teleloto." Individuals attempting to log in to these sites were required to enter their PIN1 and PIN2 codes in the SmartID app, after which all funds from their bank accounts were withdrawn and transferred to bank accounts held by foreign nationals. An increase in reports of fraud via SMS or Messenger has also been observed, where victims were informed that they had won lotteries organised by shopping centres and stores (such as "Maxima" and "Lidl"). To claim the prize, victims were initially asked to make a small payment. These messages often appeared to come from the victims' contacts on social media platforms like Facebook, and trusting these contacts, the individuals "participated" in the lottery.

It is noted that fraudsters often target specific individuals rather than random victims – typically higher-income earners – after conducting targeted searches and analyses. A large-scale case of fraud was identified in which more than €2 million in financial losses was inflicted on a company registered in Lithuania and its director. The company director received a call from an individual claiming to be a security officer from a bank operating in Lithuania, who explained that they had received information indicating the director's online banking had been infected with a "Trojan" virus. Later, the director was contacted via the mobile application WhatsApp by a man claiming to represent the Lithuanian Criminal Police Bureau. Believing the deception, the director made payments to the criminals' account and was also persuaded to transfer high-value real estate belonging to him.



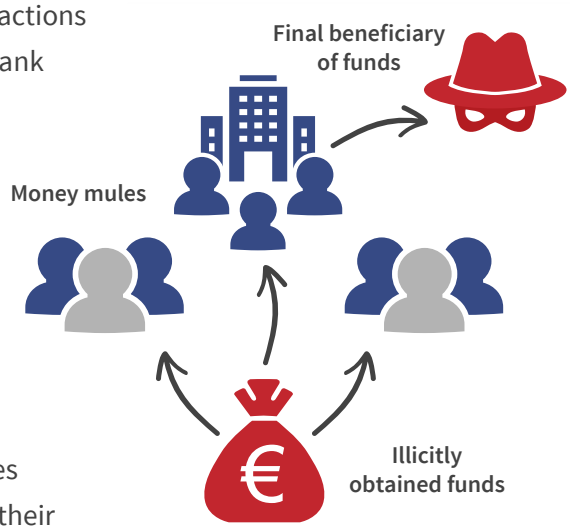
Other observable fraud trends include the use of bank accounts belonging to foreign nationals or foreign nationals with temporary residence permits in Lithuania, including students, to carry out scams. Victims report that accounts of their friends on social

networks were hacked, and they were asked to lend money to alleged friends. Many cases also involve fake advertisements: individuals transfer money for goods (usually up to €250) or event tickets but never receive them. Additionally, victims send money to purported "Alibaba" sellers but do not receive the goods.

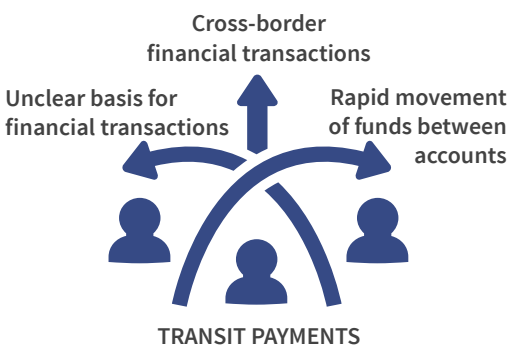
MONEY MULES

A money mule is a person who, usually for payment, receives and transfers or otherwise passes on unlawfully obtained funds to the accounts of other individuals. Such persons either open bank accounts at financial institutions for a promised fee or grant access to their existing bank accounts, which they have controlled for some time, allowing third parties to manage them. It has been observed that bank accounts are often opened with lesser-known financial institutions, where anti–money laundering and counter-terrorist financing controls may be insufficient, and remote identification is carried out. Such actions may be undertaken either knowingly, with an awareness that a criminal activity is being committed, or without understanding the illegality of the actions. Mules are recruited through job advertisements on social media or by phone, offering exceptionally attractive working conditions with minimal obligations (high pay, work from home, flexible hours). The targets are typically low-income individuals, minors, unemployed persons, or those working from home seeking additional income opportunities. The function of a money mule is to act as part of the layering chain, transferring or cashing out funds to "clean" money obtained from fraud, human trafficking, drug trafficking, or other criminal activities.

It has been observed that reports of suspicious financial transactions from financial institutions registered in Lithuania are often linked to bank accounts opened by foreign nationals (from Nigeria, the Ivory Coast) residing in European countries, used for unclear purposes. The nature of these transactions exhibits characteristics of money mule or transit accounts: payments are received from various individuals and legal entities, part of the funds are immediately transferred to other individuals' or entities' bank accounts, a portion of the received funds is retained (often up to €100), and the remainder is later withdrawn or transferred to other bank accounts belonging to the same person. This pattern of transactions reasonably indicates that the individuals receive some form of compensation for using their bank accounts to transfer funds of unclear origin.



TRANSIT PAYMENTS AND ACCOUNTS

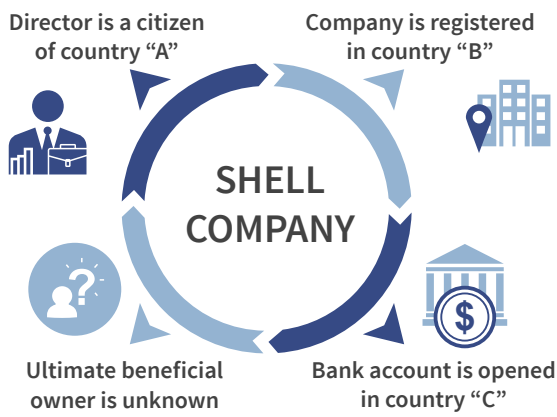


To obscure the identification of the ultimate beneficiary and the purpose of the payment, transit transfers are conducted using accounts opened with financial institutions in Lithuania. These transfers are characterised by payments between companies and individuals being executed without a clear economic rationale. Received funds are immediately transferred to another company's bank account, often involving accounts registered in other jurisdictions, thereby complicating communication between law enforcement authorities and financial

institutions. It is observed that no other types of financial operations are conducted in the bank account. The purpose of numerous transfers is ultimately to channel the funds to the de facto ultimate beneficiary, who is typically not mentioned in any company documents and is not included in the company's management or organisational structures. Transit payments and accounts are often associated with money mule activity.

SHELL COMPANIES AND COMPANY OWNERS

The activities of shell companies are closely linked to transit payments and accounts. A shell company exists legally but has no real or significant economic activity, employees, or material resources. Such companies are often established for illegal purposes – fraud, tax evasion, sanctions evasion, or asset concealment. A shell company frequently fails to submit activity declarations to the tax authorities, does not update information and data with the authority maintaining the register of legal entities, does not pay taxes, has no real place of establishment, and its registered address is often one of those where a large number of company headquarters are registered both in Lithuania and in foreign countries. There is little or no information about the company in public sources.



Funds transferred to bank accounts are immediately withdrawn in cash or transferred to other similar companies involved in the criminal chain. The recipients of funds are also engaged in vague activities such as consulting, IT, intermediary services, advertising and social media, website design, and other abstract services. Clients attempt to justify such payments using false documents, template invoices, and contracts.

A shell company owner is described as a natural person or entity formally listed as the company's owner or director, while the actual control and benefits belong to another individual. The appointment of such persons as directors is usually intended to complicate the identification of the company's true beneficiaries. This entity acts under the instructions of another person, has limited knowledge about the company, does not make strategic decisions, and lacks experience in corporate governance. Often, this is a socially or financially vulnerable person – unemployed, a student, or elderly. Public sources may indicate that the individual is listed as the owner of more than one company, usually other shell companies.

Such companies often exhibit an “international” character: the owner/director is a citizen of country A, manages the company in country B, the bank account is opened in country C, and the affected individual is a citizen of country D. Recently, reports have predominantly concerned allegedly fictitious companies registered in the United Kingdom, with owners frequently being citizens of Ukraine or Bulgaria. These companies typically have a single employee, provide IT and consulting services, receive large payments from various legal entities whose activities are also not publicly documented, immediately transfer the funds to other companies' bank accounts, cannot justify the purpose of the payments, and are unable to provide examples of the services purportedly rendered.

ILLEGAL USE OF VIRTUAL CURRENCIES

With a significant number of virtual asset service providers operating in Lithuania, alongside an increasing number of reports on suspicious financial transactions, the use of virtual currencies for illicit purposes is also rising. Individuals conduct transactions on the dark web using virtual currency addresses linked to narcotics, child sexual abuse material, the distribution of payment card data, terrorist financing, or other virtual currency addresses subject to international sanctions. Large transfers are made without the ability to justify the source of the funds.

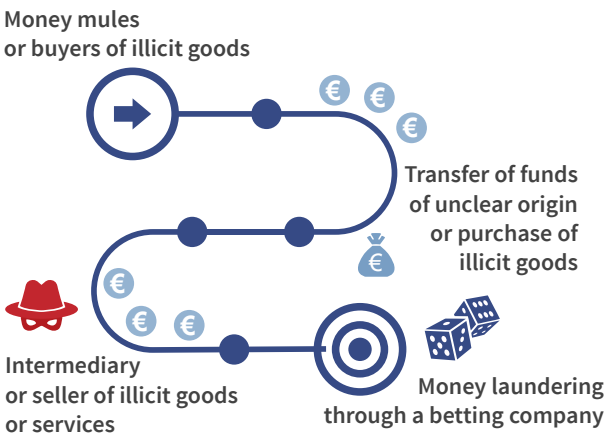
Dark web marketplaces typically accept payments in virtual currencies to preserve the anonymity of both the seller and the buyer, facilitate transactions across different jurisdictions, and thereby complicate the traceability of funds. For these reasons, individuals seeking to use such marketplaces must first acquire virtual currency. Various methods are employed to maintain their anonymity: using a VPN, creating accounts in the names of third parties, using fake documents, and employing concealment/mixing services. While mixing services are not inherently illegal, they are often used to obscure the origin of funds and complicate the traceability of transactions linked to dark web marketplaces, cybercrime, fraud schemes, or sanctions evasion.

It should be noted that the use of virtual currencies is also significant when examining investment fraud schemes – victims' funds are transferred immediately from traditional bank accounts to virtual -asset service providers' platforms, often using accounts set up by money mules or employing false documents. Funds are routed through multiple addresses to hinder traceability. The chain frequently involves virtual currency exchange platforms operating in different jurisdictions, aiming to fragment the flow of funds and complicate oversight.

OTHER CRIMES AND LEGAL VIOLATIONS

A high volume of financial transactions to and from betting companies' accounts may be linked to the trade of narcotic and psychotropic substances or other illegal activities. Analysis of received reports has shown that young individuals are making payments into betting companies' accounts. Payments are made continuously in small amounts, usually up to €50. Funds are often received from different individuals in rounded amounts (e.g., €20, €30, €50) and are immediately transferred to betting company platforms. The origin of these funds and the purpose of the payments remain unclear; however, based on the overall data, in some cases it is suspected that individuals are trading narcotic or psychotropic substances and subsequently using the betting platforms to launder the proceeds as “winnings.” In some cases, due to the suspected criminal activity of the individual, pre-trial investigations have already been initiated, or it has been established that in the past the individuals involved—or those making the transfers—were held criminally liable under Article 259 of the Criminal Code of the Republic of Lithuania (illegal

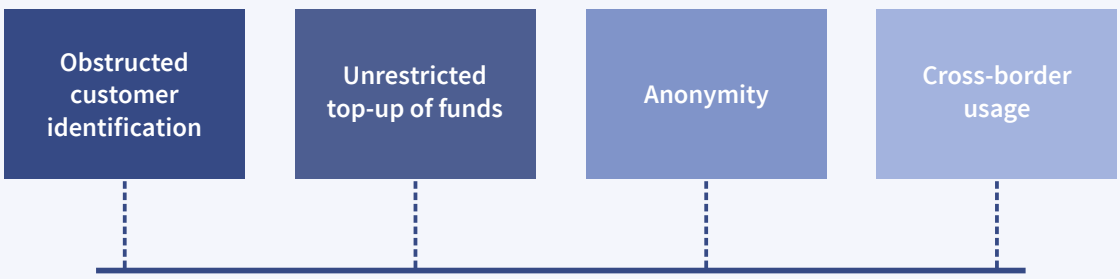
possession of narcotic or psychotropic substances without the intent to distribute) and/or Article 260 (illegal possession of narcotic or psychotropic substances with the intent to distribute, or illegal possession of a very large quantity of such substances). In one analysis, it was found that the individual received nearly €40,000 over a short period from 191 persons, mostly with the payment purpose indicated as "play," "transfer," or "game." In this case, a large portion of the funds was eventually withdrawn in cash, and it was also established that a pre-trial investigation had already been initiated under Article 260, Part 1 of the Criminal Code of the Republic of Lithuania.



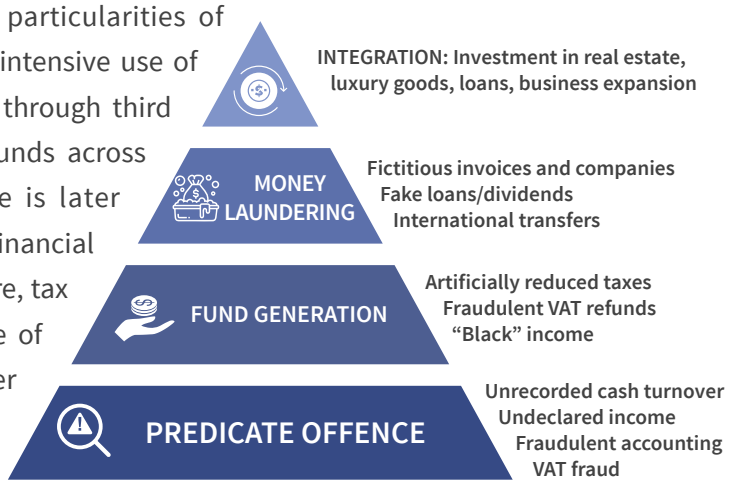
Financial institutions reported the possible use of a client's bank account for handling and laundering funds suspected to have been obtained from prostitution or human trafficking. In all analyses, clients raised suspicion not only because of the nature of the suspicious financial transactions, but also because, at the time of establishing the business relationship, the telephone number provided by the client was publicly listed and also used on goods and services advertisement portals offering sexual services, as well as on various escort websites. Analysis of the subjects' financial transactions shows that payments are made to websites containing adult content advertisements and escort service promotions, with funds received from third parties, mostly under male names. Payments are typically in round amounts, made late at night and/or during the night. The accounts are used internationally, with funds either withdrawn from ATMs or transferred via fast money transfer platforms.

Information has been received regarding potential money laundering involving prepaid payment cards. Unlike debit or credit cards, a prepaid payment card is not directly linked to a bank account and can often be issued with limited customer identification, funded with cash or through money mule bank accounts, as well as stolen cards, which makes it difficult to identify the actual card user.

These are consumer top-up prepaid cards intended for daily expenses, shopping, and leisure activities. Reports have been received concerning high-risk third-country nationals residing in France, whose suspicious financial activity includes loading prepaid cards with vouchers, followed by cryptocurrency purchases and/or financial transactions via various money transfer platforms. In many cases, inquiries were received from French law enforcement authorities regarding the institution's clients, given that pre-trial investigations were initiated on suspicion that the subjects may be involved in fraudulent activities.



Tax-related crimes involve illegal actions aimed at avoiding tax payments, unlawfully reducing tax liabilities, or reclaiming taxes—most often by providing false information to the tax authority or concealing the true economic activity. Such conduct may include unreported income or turnover, the use of fictitious transactions or documents, artificially inflating expenses, disguising employment relationships, as well as creating complex domestic or international structures to shift profits or hide taxable income. A common form of tax crime is the illegal application or reclaiming of value-added tax, where formally declared transactions do not reflect real economic activity or exploit the particularities of international trade. Tax crimes are often linked to intensive use of cash, the splitting of money flows, intermediaries through third parties or affiliated companies, and transfers of funds across different jurisdictions. Illegally obtained income is later integrated into the financial system through various financial instruments, consumption, or investments. Therefore, tax crimes are considered a significant primary source of criminal activity, forming a foundation for further money laundering.



Terrorist financing encompasses any direct or indirect actions through which funds or assets are collected, accumulated, transferred, or otherwise managed, knowing or suspecting that they may be used to support terrorist acts, terrorist organisations, or individual persons involved in terrorism. Terrorist financing can involve both illicit and fully legitimate funds, which is why such activity is often disguised as ordinary economic, charitable, or personal financial transactions. The movement of funds typically involves small transfers, splitting of amounts, short holding periods, the use of intermediaries or third parties, and payments across multiple jurisdictions to complicate the identification of the ultimate beneficiaries. Various financial and non-financial instruments can also be used for terrorist financing, including cash, prepaid payment cards, or virtual currencies, which facilitate rapid and hard-to-trace transfers of funds.

Splitting of funds and small transactions

Funds of both legal and illegal origin

Use of different jurisdictions and intermediaries

Obstructed traceability of financial transactions

Reports are received from obliged entities concerning possible client links to terrorist groups or terrorist financing, where clients make transfers to virtual currency addresses identified as associated with terrorist organizations and their funding. Information on suspicious client activity is also identified through the analysis of open sources and publicly available information, revealing connections and potential specific financial transactions supporting terrorist organizations. During this period, information was also received regarding the use of a Lithuanian IBAN account for the purchase and payment of goods that were subsequently used to carry out a terrorist attack abroad. However, the financial transactions posing the highest risk are usually detected only after receiving an inquiry from a law enforcement authority regarding a client, or following the emergence of publicly available information on individuals suspected of terrorist financing and/or involvement in terrorist attacks.

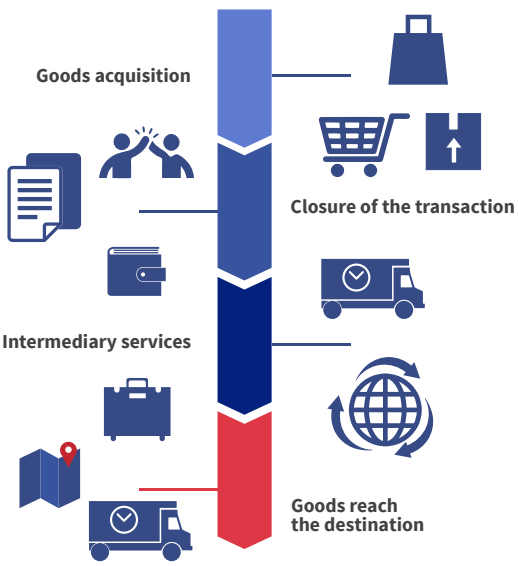
CURRENT TYPOLOGIES OF INTERNATIONAL SANCTIONS EVASION

During the reporting period, the following principal typologies of international sanctions circumvention were identified.

Circumvention of sanctions through the sale of luxury vehicles. High-end cars are sold via third countries, transported in maritime containers around Europe, or disguised as personal property within commercial shipments. Methods used to deliver luxury vehicles to Russia are continuously evolving, adapting to changing circumstances and regulatory environments. Lithuanian legal persons engaged in the automotive trade, which prior to the imposition of sanctions on the Russian Federation and the Republic of Belarus conducted business with these jurisdictions, have established cooperation with new partners in Kazakhstan, Uzbekistan, Kyrgyzstan, Turkey, and Georgia. These countries are deliberately incorporated into supply chains as intermediary jurisdictions. As a result, goods sold by Lithuanian entities—namely passenger vehicles and heavy goods vehicles—ultimately continue to reach the sanctioned markets of the Russian Federation and the Republic of Belarus, notwithstanding the applicable sanctions regime.

It should be noted that vehicles are being sold to citizens of the Russian Federation and the Republic of Belarus for amounts below EUR 50,000, whereas the average market value exceeds EUR 50,000. In this manner, Lithuanian legal persons acquire vehicles at a value exceeding EUR 50,000 and subsequently sell them at a lower price. It is observed that the goods predominantly consist of luxury passenger vehicles and heavy goods vehicles. Sectoral sanctions breaches are likewise prevalent in transactions involving legal or natural persons of the Kyrgyz Republic, the Republic of Uzbekistan, and the Republic of Belarus. A proportion of the goods sold, upon verification through publicly available sources, are identified within a short period (1–3 months) as having been registered in the Russian Federation.

CIRCUMVENTION OF SANCTIONS THROUGH THE SALE OF DUAL-USE GOODS AND TECHNOLOGIES



Circumvention of sanctions through the sale of dual-use goods and technologies. The majority of entities involved are companies registered in Lithuania that have long-standing experience in trade with Russian or Belarusian entities. Russia has developed a broad network of companies used as a cover for sanctions evasion and is systematically expanding it. Intermediary companies facilitating transactions for Russian entities are established in countries that do not support the EU, UK, or US sanctions policy. Companies in these jurisdictions seek various ways to obtain the required equipment.

In order to circumvent existing financial sanctions, intermediary entities registered in third countries such as Kazakhstan, Turkey,

Kyrgyzstan, Uzbekistan, and the United Arab Emirates are involved. Although these countries are not directly subject to sanctions, goods may be imported or exported through them. As in previous years, payments by Lithuanian legal entities to newly established foreign companies that are not the final recipients of goods continue to be observed. These companies are typically newly registered, do not possess their own assets, sell products that are not typical for their stated operational region, and in some cases relocate their activities to new jurisdictions.

In this way, newly established companies are used to avoid applicable sanctions, and goods reaching countries friendly to the Russian Federation ultimately reach Russia itself. In many cases, Lithuania functions as a re-exporting country, where businesses act either as intermediaries or freight forwarders. By using intermediary countries, attempts are made to circumvent sanctions applied to exported goods that could enhance the Russian military and its technologies or support the development of the defence and security sector.

It is observed that economic operators involved in the chain of purchase, sale, and delivery of goods deliberately conceal the country of origin of the products. Such practices are typically associated with an attempt to reduce the level of scrutiny (avoiding customs inspections or attracting less attention from banks when receiving or executing payment transfers), circumvent restrictions on specific goods subject to rules of origin limitations, and create a misleading impression of transparency within the supply chain, particularly where the origin of goods is a key criterion for the application of sanctions.

Falsification of documents.

Multiple instances have been identified in which legal persons, seeking to carry out the export or import of goods, submit falsified letters, forged contracts, certificates of origin, and other documentation to the Lithuanian Customs authorities and the Service. In many cases, such fraudulent documents are signed by legal entities registered in foreign jurisdictions, which limits the ability of competent authorities to effectively enforce liability for document forgery.

Use of legal entities (intermediaries) operating in other jurisdictions.

It is established that, in order to supply sanctioned goods to Russia or Belarus, such goods are first sold to legal entities incorporated in other jurisdictions, after which they are re-exported to the Russian Federation or the Republic of Belarus.

Use of euro banknotes.

During the reporting period, instances of the unlawful transportation of euro banknotes to the Russian Federation and the Republic of Belarus were identified.

Use of sanctioned banks.

A significant number of cases continue to be identified in which Lithuanian entities maintain accounts with sanctioned banks and conduct operations through them, including money transfers, currency exchanges, and cash withdrawals.

Establishment of new subsidiary companies in third countries.

Sanctions restricting the acquisition of certain categories of goods (e.g. timber, metal products, aviation parts) are encouraging business operators to establish subsidiaries outside the European Union. During the reporting period, it has been observed that Lithuanian citizens or individuals holding residence permits in the Republic of Lithuania also contribute to the establishment of such entities. In this way, goods are imported into Lithuania via third countries, concealing their origin and circumventing direct sanctions. These cases are further complicated by a lack of traceability in transport routes. For example, an analysis has shown that a Lithuanian-registered legal entity sells its own manufactured goods (subject to sanctions) to a subsidiary company in Poland, which then resells them to another subsidiary of the Lithuanian legal entity in Belarus. In such cases, it is difficult to determine whether sanctions are being breached in the course of the sale and subsequent re-export of goods.

Transit of sanctioned goods through the territory of Lithuania.

Within the logistics and transit sector, situations have been identified in which the indirect owners or sellers of goods transported in transit through Lithuania are sanctioned persons, while Lithuanian logistics companies provide services related to the logistics, warehousing, and customs brokerage of such goods.

Provision of logistics services.

An increase in the involvement of Lithuanian logistics companies in sanctions circumvention schemes has been observed. Logistics companies fail to ensure compliance with sanctions requirements and organise and transport sanctioned goods. In many cases, attempts are made to rely on formal contractual clauses regarding the implementation of sanctions requirements, often shifting the burden to the customer (e.g. a Belarusian company) or stating that the goods are not sanctioned, that the manufacturer complies with sanctions requirements, or that exemptions apply (for example, goods exported before the end of the transitional period specified in the regulation). However, no real checks or effective sanctions compliance measures are undertaken. Companies often shift responsibility for the potential transport of sanctioned goods to Lithuanian customs authorities, claiming that customs allowed the shipments to pass. There are also cases where responsibility is attributed to the state-owned company Lietuvos Geležinkeliai when goods are transported by rail.

In this way, companies seek to avoid liability for possible sanctions violations and transfer the entire burden of sanctions compliance to Lithuanian institutions and state-owned entities.

International public procurement.

A case has been identified in which an entity associated with a sanctioned party participated in international public procurement procedures, thereby circumventing applicable restrictions and restrictive measures (sanctions).

Use of services provided by a sanctioned Russian funds.

Actions have been identified whereby individuals facilitated the circumvention of financial institutions controlled by the competent authorities of the Member States of the European Union, thereby enabling the receipt of funds from a sanctioned Russian fund while avoiding the freezing of assets.

05

SUPERVISION OF OBLIGED ENTITIES

The Money Laundering Prevention Board, in the exercise of its assigned functions, also carries out supervision of financial institutions and other obliged entities, with the aim of ensuring compliance with anti-money laundering and counter-terrorist financing requirements.

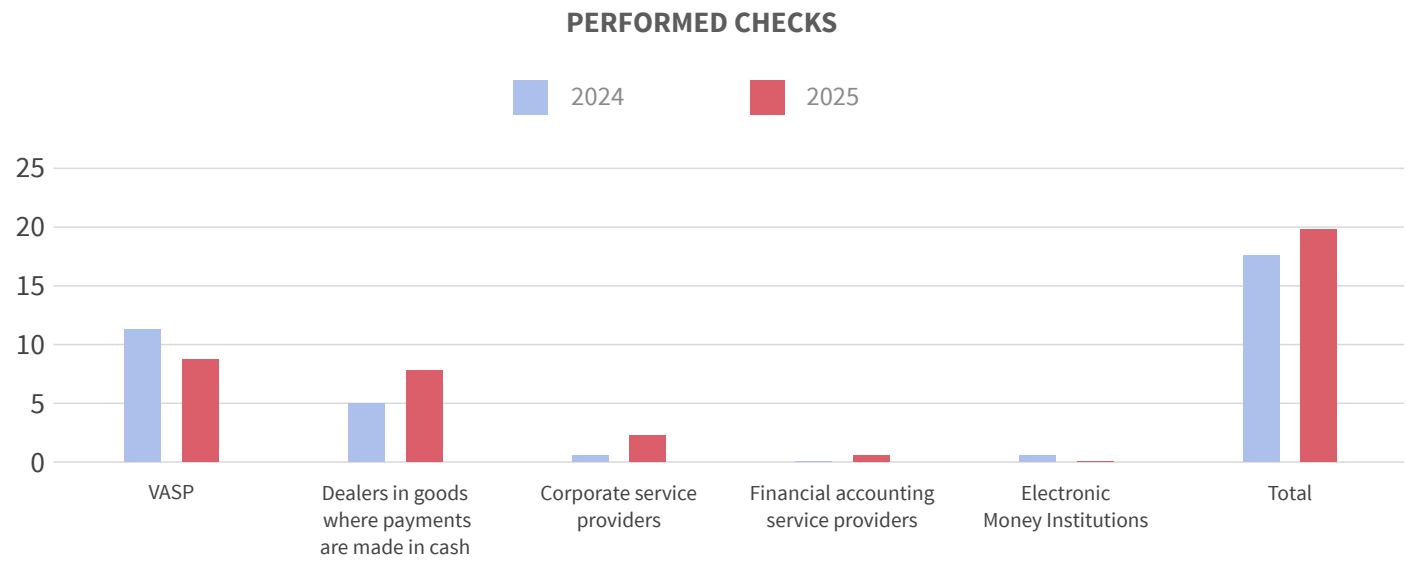
Within the Board, these functions are performed by the Supervision Division, whose principal responsibilities include the supervision of financial institutions and other obliged entities, as well as the conduct of strategic sectoral analyse.

SUPERVISION OF FINANCIAL INSTITUTIONS AND OTHER OBLIGED ENTITIES

In the official memorandum No. 4-667 of 21 January 2025 of the Supervision Division of the MLPB, and in accordance with the Procedure Description for inspections of economic operators carried out by employees, approved by Order No. 46-V of 10 May 2008 (as amended by No. V-243 of 30 December 2024), six companies were included in the list whose scheduled inspections were to be carried out in 2025. Other inspections conducted in 2025 were unscheduled.

The Supervision Division carried out 20 inspections of obliged entities in 2025.

In 2025, the Supervision Division carried out a total of 20 inspections of obliged entities, of which 9 companies were engaged in the activity of custodial virtual currency wallets and virtual asset service providers. By comparison, in 2024 a total of 18 inspections of obliged entities were carried out, of which 11 companies were engaged in VASP activities.



In 2025, following inspections of 10 companies, breaches were identified relating to customer due diligence and verification requirements, reporting of suspicious monetary transactions or operations, and the review of complex, unusually large or unusually structured transactions. Further deficiencies were found in record-keeping obligations, reporting of transactions exceeding EUR 15,000, appointment and training of responsible employees, designation of senior management responsibility, and the establishment of internal policies and internal control procedures.

NATURE OF VIOLATIONS IDENTIFIED DURING INSPECTIONS

Customer identification and due diligence requirement breaches	7	Violations in reporting transactions of EUR 15,000 and above	4
Violations of reporting suspicious transactions or operations	2	Violations in appointment and training of responsible staff	5
Failures in examining complex, unusually large or unusual structured transactions	2	Violations in the appointment of a senior executive	3
Violations of information retention requirements	6	Violations in establishing internal policies and internal control procedures	6

ANALYSIS OF ACCOUNTING AND TAX ADVISORY SERVICE PROVIDERS' ACTIVITIES IN LITHUANIA

In 2025, the Supervision Division of the MLPB conducted a sectoral analysis of the accounting and tax advisory services sector entitled “Prevention of money laundering, its effectiveness and potential risks”. This sectoral strategic analysis covers the activities of legal entities providing financial accounting or tax advisory services, as well as individuals providing such services independently, and persons who, in the course of their principal business or professional activity, undertake—directly or through other persons with whom they are associated—to provide material assistance, support, or advice on tax matters (hereinafter referred to as accounting or tax advisory service providers). The analysis examines the applicable legal framework, the money laundering risk factors associated with such entities, and other aspects related to the provision of accounting and tax advisory services in Lithuania, with the aim of assessing the scope of this activity and its risk profile in terms of money laundering.

The analysis aimed to assess whether accounting and tax advisory service providers, which have been designated as obliged entities since 2004, are familiar with anti-money laundering measures and implement them in practice. It also sought to enable the Service, as the supervisory authority, to identify, assess, and understand the overall money laundering risk within the sector and to take the necessary AML measures to ensure that such risks are effectively and efficiently mitigated and managed. Although accounting and tax advisory service providers have been classified as obliged entities since 2004 and are therefore required to implement AML measures – creating the impression that the sector is well acquainted with AML requirements and applies them effectively – the findings of both the Second National Money Laundering and Terrorist Financing Risk Assessment (2015–2018) and the Third National Money Laundering and Terrorist Financing Risk Assessment (2019–2022) demonstrated that the activities of accounting professionals and tax advisers in Lithuania pose a high risk of money laundering (and were assessed together with auditors as a single sector).

The analysis states that financial accounting professionals play an important role in identifying and preventing financial crime, as they manage financial records, transactions, and tax declarations. Tax advisers likewise play a significant role by providing guidance on taxation, including calculation, declaration, payment, reliefs, and other related matters. Due to the nature of their functions, accounting and tax advisory service providers have a genuine capacity to protect the state financial system from criminal activities related to money laundering and illicit financial operations. Regardless of whether services are provided within a large company or by an individual practitioner, the failure to recognise activities that may be linked to money laundering, as well as a lack of knowledge on how to respond in such

cases, poses a significant money laundering risk and increases the likelihood that such services may be exploited for illicit purposes.

USE OF "STRIX AML" SOFTWARE

The Service, in the course of supervising the implementation of anti-money laundering and counter-terrorist financing measures, in February 2025 submitted questionnaires to VASP entities related to the implementation of measures for the prevention of money laundering and/or terrorist financing submitted to the Service. Invitations to participate in the survey were sent to 667 companies that carried out VASP activities in 2024. The data obtained by aggregating all completed questionnaires is not publicly available. In 2026, it is planned to issue questionnaires on information related to the implementation of anti-money laundering and/or counter-terrorist financing measures to real estate agents (brokers) and providers of financial accounting or tax advisory services.

On 15 December 2025, the Service submitted a request to VASP entities via the "Strix" platform to complete a questionnaire regarding the cessation of their activities. The questionnaire requests information on whether the entities hold licences in other European Union Member States, the plans of entities that will not seek a licence after 1 January 2026, the companies' need to submit STR/CTR reports after the end of the transitional period, details of persons appointed by the companies responsible for cooperation with the FCIS after 1 January 2026, and other relevant information.

MEASURES IMPOSED ON OBLIGED ENTITIES

In 2025, the Commission for the Examination of Violations of the Law on the Prevention of Money Laundering and Terrorist Financing of the Republic of Lithuania reviewed 13 sets of inspection material concerning obliged entities. Following the assessment of this material, 11 companies were subject to enforcement measures, including monetary fines ranging from EUR 2,435.12 to EUR 771,400, as well as one mandatory instruction. In total, in 2025, fines imposed on other obliged entities for breaches of the LPMLTF amounted to EUR 1,455,912.27. By comparison, in 2024, 11 sets of inspection material were reviewed, resulting in total monetary fines of EUR 1,813,323.36.

In 2025, the Supervision Division of the MLPB represented the Service in 14 court proceedings related to violations of anti-money laundering and counter-terrorist financing prevention requirements.

In 2025, fines imposed on other obliged entities for breaches of the LPMLTF amounted to EUR 1.45 million.

FATF Recommendations R27, R28 and R35 on the effective implementation of supervisory standards establish that supervisory authorities should apply a sufficiently broad range of sanctions and other measures designed to address identified deficiencies and to ensure that sanctioned obliged entities achieve sustained future compliance. On this basis, effective remedial actions and enforcement measures should not only deter past non-compliant behaviour and correct deficiencies in the processes, procedures, systems, or controls of regulated entities, but also promote behavioural change aimed at fostering a culture of compliance encompassing the Board, senior management, compliance functions, and all other relevant employees within the entity. In order to achieve this objective, changes are planned within the division's activities regarding the monitoring of the remediation of LPMLTF breaches identified during inspections of obliged entities.

COOPERATION

Pursuant to the agreement signed on 25 November 2024 between the Service and the Bank of Lithuania, the Service provided the Bank of Lithuania with 17 certificates concerning VASP profile companies that had applied to the Bank of Lithuania for the issuance of a crypto-asset service provider licence.

In accordance with the same agreement, the Service and the Bank of Lithuania carried out four joint VASP inspections in 2025.

On 30 June 2025, a visit of Moldovan officials took place in Vilnius, during which information and experience were exchanged on VASP regulation, typologies of suspicious transactions, the implementation of measures for the prevention of money laundering and/or terrorist financing, and the supervision of international financial sanctions.

In addition, an information notice for VASPs was published on the Service's website regarding the strengthening of VASP supervision until the end of 2025 and the mandatory requirement to obtain a crypto-asset service provider licence from 1 January 2026.

06

LEGISLATION

Draft regulatory technical standards (RTS) are being prepared. They aim to create a clear and uniform framework for the prevention of money laundering and terrorist financing across the EU.

On 31 May 2024, the European Union anti-money laundering and counter-terrorist financing legislative package entered into force, aimed at establishing a unified, risk-based, and more effective system for combating money laundering across the EU. The package consists of Regulation (EU) 2024/1624 on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing, Directive (EU) 2024/1640 on the mechanisms to be put in place by Member States, and Regulation (EU) 2024/1620 establishing the Anti-Money Laundering and Countering the Financing of Terrorism Authority (AMLA).

To ensure consistent application of these legal acts, the European Banking Authority (EBA) is developing draft Regulatory Technical Standards (RTS), which provide detailed practical aspects of implementation. The RTS package consists of several interrelated draft standards covering the risk assessment of obliged entities, the selection of entities for supervisory purposes, customer due diligence (CDD) requirements, and the application of sanctions and other enforcement measures. These standards are intended to establish a clear and uniform anti-money laundering and counter-terrorist financing framework across the European Union.

In 2025, these draft RTS reached the stage of public consultation and coordination. National authorities, including financial intelligence units, were involved in this process and provided comments and proposals regarding the practical application of the requirements. This created the basis for ensuring that the forthcoming standards would be aligned both with EU-level objectives and with the specific features of national systems.

It also participated in the activities of the AMLA General Board in its FIU composition, where documents related to FIU operations are discussed and adopted (including joint analyses, peer reviews, and similar outputs), as well as in meetings of AMLA expert network working groups on the drafting of Regulatory Technical Standards (RTS), to which written comments were submitted.

AMENDMENTS TO THE LAW ON THE PREVENTION OF MONEY LAUNDERING AND TERRORIST FINANCING OF THE REPUBLIC OF LITHUANIA

In 2025, the MLPB actively participated in the drafting of amendments to the LPMLTF, the purpose of which is to implement the Regulation (EU) 2024/1620 of 31 May 2024 establishing the Anti-Money Laundering and Countering the Financing of Terrorism Authority and amending Regulations (EU) No 1093/2010, (EU) No 1094/2010, and (EU) No 1095/2010 (hereinafter – Regulation (EU) 2024/1620). The aim of the amendments is to align the existing national regulatory framework with the provisions of Regulation (EU) 2024/1620 governing the functions of the European Union Anti-Money Laundering and Countering the Financing of Terrorism Authority (AMLA), to establish procedures for the implementation of the rights granted to this authority in Lithuania, and to enhance the Republic of Lithuania's economic competitiveness, foreign direct investment attraction, and opportunities for domestic investor development.

On 25 June 2025, the Law of the Republic of Lithuania on the Prevention of Money Laundering and Terrorist Financing No. VIII-275, amending Articles 2, 4, 5, 6, 7, 8, 9, 10, 15, 22, 23, 26, 27, 28, 29, 39, 40, 42 and its Annex, and supplementing it with Article 32[1], introduced the following key changes:

- strengthened cooperation and information exchange between the Service and other national institutions with the EU-level AMLA;
- a transition from a detailed and formal regulatory approach to a more flexible, risk-based model for customer and beneficial owner identification;
- simplified customer due diligence requirements in low-risk cases, particularly within the financial sector;
- improved conditions for the operation of financial institutions, innovation, and the adoption of technological solutions while maintaining the effectiveness of AML/CFT measures;
- enhanced Lithuania's economic competitiveness, investment attractiveness, and financial sector development;
- established a financing mechanism for AMLA operations and defined the payment procedure for supervised financial institutions;
- regulated the procedure for issuing court authorisations for on-site inspections when carried out in residential premises.

ORDERS OF THE DIRECTOR OF THE SERVICE

In order to properly organise the anti-money laundering and counter-terrorist financing activities carried out by the MLPB and to enhance the effectiveness of the supervision of the implementation of preventive measures, the following legal acts were approved by orders of the Director of the Service:

- by Order No. V-54 of 27 February 2025, instructions were approved for legal entities providing financial accounting or tax advisory services, individuals providing such services independently, and persons who, in the course of their principal business or professional activity, undertake—directly or through other persons with whom they are associated—to provide material assistance, support, or advice on tax matters, aimed at preventing money laundering and/or terrorist financing;
- by Order No. V-125 of 23 May 2025, instructions were approved for legal entities providing financial accounting or tax advisory services, individuals providing such services independently, and persons who, in the course of their principal business or professional activity, undertake—directly or through other persons with whom they are associated—to provide material assistance, support, or advice on tax matters, aimed at preventing money laundering and/or terrorist financing;
- by Order No. V-126 of 23 May 2025, instructions were approved for real estate agents (brokers), both acting on behalf of and for the benefit of clients, and assisting clients in carrying out real estate purchase or sale transactions and/or related transactions, as well as providing intermediary services in the leasing of real estate, but only in cases where the monthly rent is equal to or exceeds EUR 10,000 or an equivalent amount in foreign currency, with the aim of preventing money laundering and/or terrorist financing;
- by Order No. V-162 of 8 July 2025, the Procedure Description for the exchange of information concerning a customer and their representative, the customer's beneficial owner, persons involved in the ownership and control structure of a corporate customer, and/or monetary transactions or operations was approved;
- by Order No. V-221 of 16 September 2025, instructions were approved for trust or company formation and administration service providers, aimed at preventing money laundering and/or terrorist financing.

07

IMPLEMENTATION OF INTERNATIONAL SANCTIONS

In implementing international financial sanctions, the MLPB undertook the following actions:

- granted 339 exemptions or authorisations to disapply restrictions and obligations set out in legal acts establishing international sanctions;
- provided continuous consultations by email and telephone to natural and legal persons, as well as to state institutions, on the implementation of international sanctions;
- collected and maintained statistical information on the implementation of international sanctions within the Service;
- submitted reports to the Ministry of Foreign Affairs of the Republic of Lithuania on sanctions implementation (monthly and quarterly reports);
- collected, maintained, and published statistical information on frozen funds and assets located in the Republic of Lithuania and belonging to sanctioned persons;
- organised and delivered four training sessions on the implementation of international sanctions in the Republic of Lithuania;
- received 232 reports from financial institutions concerning possible sanctions circumvention or evasion cases; carried out analyses of 77 reports and forwarded part of them to other competent Lithuanian and EU authorities;
- updated and supplemented the FAQ section;
- initiated and examined administrative offence cases concerning violations of international sanctions, in which the MLPB Supervision Division issued 27 decisions and imposed monetary fines totalling EUR 32,150 (for comparison, in 2024, 20 administrative offence cases concerning violations of international sanctions were examined, resulting in 19 decisions and total fines of EUR 28,000);
- the MLPB Supervision Division participated in 7 court proceedings related to decisions in administrative offence cases concerning violations of international sanctions;
- the MLPB Compliance Division participated in 44 court proceedings related to the Service's administrative decisions in the field of international sanctions implementation, including decisions on the application of enforcement measures against legal persons for violations of international sanction;
- the MLPB Compliance Division also participated in 5 proceedings before courts of general jurisdiction related to the application of international sanctions, in which it provided 6 opinions on the application of international sanctions and 2 submissions in cases where the FCIS was involved as a third interested party;
- participated in Court of Justice of the European Union (CJEU) proceedings in preliminary ruling cases referred by Lithuanian courts, including attendance at the hearing in case C-84/24 and the preparation of draft positions and assessments in cases C-147/25, C-412/25, and C-635/25;
- prepared two national positions for CJEU cases in which Lithuania submitted observations (through the Ministry of Justice);
- organised and participated in meetings of the International Sanctions Implementation Commission, which in 2025 initiated 45 inspections, applied enforcement measures in 12 proceedings, issued one written order, and imposed fines totalling EUR 6,236,375.46.

The International Sanctions Implementation Commission has imposed fines totalling EUR 6.23 million

NUMBER OF EXAMINED ADMINISTRATIVE OFFENCES

2023	2024	2025
12	20	29

CONTENT OF IDENTIFIED ADMINISTRATIVE OFFENCES

Violations in the execution of international public procurement	1
Failure to provide information	1
Performance of actions enabling the circumvention of controls applied by financial institutions supervised by authorities of European Union Member States	5
Use of services of EU-sanctioned banks	20

08

COUNCIL OF EUROPE EXPERTS (MONEYVAL) ASSESSMENT

In 2025, preparations were initiated for the Council of Europe's Committee of Experts on the Evaluation of Anti-Money Laundering Measures and the Financing of Terrorism (MONEYVAL)) 6th-round mutual evaluation of Lithuania. The evaluation will assess the effectiveness of Lithuania's anti-money laundering and counter-terrorist financing system and its compliance with FATF standards.

It is planned that in autumn 2026, preparatory training will be organised for representatives of Lithuanian institutions to familiarise them with the procedures of the MONEYVAL 6th round evaluation. In spring 2027, technical questionnaires will be completed, and in autumn 2027 an on-site evaluation visit by MONEYVAL experts is planned in Lithuania. In May 2028, the Lithuanian evaluation report is expected to be considered and adopted at the plenary session.

WORKING GROUP ON THE COORDINATION OF ANTI-MONEY LAUNDERING AND COUNTERING THE FINANCING OF TERRORISM ACTIVITIES

In 2025, the MLPB organised two meetings of the Working Group (hereinafter – the Working Group), established by Order No. 154 of 2 May 2013 of the Prime Minister of the Republic of Lithuania “On the Establishment of the Working Group” (hereinafter – the Order).

At one of the Working Group meetings (November 2025), the Head of the Latvian Financial Intelligence Unit participated and presented the challenges faced by Latvia in preparing for the 6th-round MONEYVAL assessment of Latvia's progress, as well as sharing good practices.

In order to properly prepare for the upcoming evaluation under the FATF methodology, a table containing the FATF Recommendations and effectiveness indicators was submitted to the Working Group members for coordination, indicating the institutions responsible for their implementation.

09

MEASURES TO MITIGATE MONEY LAUNDERING AND TERRORIST FINANCING RISKS

Following the publication of the third National Money Laundering and Terrorist Financing Risk Assessment (hereinafter – NRA), which is conducted every four years and covers the 2019–2022 period, and after evaluating its results, the Working Group approved, on 7 April 2025, the Action Plan on Measures to Mitigate Money Laundering and Terrorist Financing Risks of the Republic of Lithuania for 2025–2027 (hereinafter – the Plan), with the aim of reducing the identified risks.

The Plan sets out 62 measures, the implementation of which is assigned to the competent authorities of the Republic of Lithuania specified therein (ministries, supervisory authorities of obliged entities, law enforcement and other state institutions). The MLPB is responsible for the implementation of 19 measures set out in the Plan.

In 2025, the MLPB implemented measures included in the Plan relating to methodological assistance (training on anti-money laundering and terrorist financing prevention, as well as international sanctions implementation, provided to financial institutions and other obliged entities; preparation and publication of information notices; updating of FAQs), supervision of financial institutions and other obliged entities (including on-site inspections), analytical activities (analysis and synthesis of STR data, identification of typologies of financial transactions and sanctions evasion), and improvement of STR reporting forms. As foreseen in the Plan, the MLPB also participated in the activities of AMLA working group.

10

PARTICIPATION IN INTERNATIONAL-FORMAT MEETINGS

ACTIVITIES OF THE EGMONT GROUP

In 2025, representatives of the Lithuanian Financial Intelligence Unit continued to participate in the activities of the Egmont Group – an international network uniting 182 financial intelligence units, dedicated to the secure exchange of financial intelligence and the fight against money laundering and terrorist financing.

Lithuania's membership in this organisation is based on the Egmont Group Charter, which the Service signed on 31 May 2007.

From 6 to 11 July 2025, the 31st Egmont Group Plenary Session was held in Luxembourg, during which the updated Information Exchange Working Group (IEWG) Action Plan for 2025–2026 was approved. The meetings placed particular emphasis on strengthening the operational independence and autonomy of financial intelligence units. The document "FIU Operational Independence and Autonomy" was adopted, establishing 18 core principles to become an integral part of the Egmont Group Charter.

The implementation of these principles becomes a mandatory requirement for both new and existing members. A three-year transitional period (2025–2028) has been foreseen, after which, depending on the level of compliance, conformity or support procedures may be applied. Such procedures may be initiated either during assessments, upon receipt of observations from other member states, or following significant changes in national systems.

In commemoration of the 30th anniversary of the Egmont Group, a decision was taken to mark 9 June annually, starting from 2026, as the International Financial Intelligence Units Day. In 2025, new member states also joined the Egmont Group – Mozambique, The Gambia, Equatorial Guinea, Sierra Leone, and Nauru – further expanding the global financial intelligence cooperation network.

June 9th is International Financial Intelligence Unit Day.

ACTIVITIES OF THE COUNCIL OF EUROPE COMMITTEE OF EXPERTS (MONEYVAL)

In 2025, two MONEYVAL plenary sessions were held, in which a representative of MLPB participated as head of the Lithuanian delegation. The sessions addressed international anti-money laundering and counter-terrorist financing issues, updates to procedures, and emerging risks, and adopted the evaluation report of Latvia – the first under the new assessment cycle. At the 70th session, the MONEYVAL work programme for 2026 was also approved, including preparatory training for Lithuania ahead of the 6th evaluation round.

At the 70th session, the MONEYVAL work programme for 2026 was approved.

MONEYVAL project "Typologies Project Report: Money Laundering, Terrorism Financing and Proliferation Financing Risks and Trends Linked to Proceeds Obtained from Conflicts". In 2025, the typologies report was successfully completed and approved at a MONEYVAL plenary session. MLPB representatives actively contributed to the preparation of the report. The objective of the analysis was to assess how illicit proceeds generated in regions affected by armed conflicts and/or military aggression are obtained, how these proceeds are laundered, and how they are used to finance terrorism and the proliferation of weapons of mass destruction, as well as how such risks can be mitigated through improved understanding of the issue and enhanced coordination of the response.

FIU PLATFORM

In 2025, representatives of the Lithuanian Financial Intelligence Unit actively participated in the activities of the Financial Intelligence Units Platform (FIU Platform). Four meetings of the platform were held during the year. The meetings addressed topical issues related to information exchange, strengthening of cooperation, and the implementation of new technological solutions.

Particular attention was given to the updated FIU.net ("Next Generation FIU.net") system, which enables more efficient, secure, and faster exchange of data between EU financial intelligence units and strengthens cross-border cooperation in combating financial crime and investigating complex cross-border financial criminal schemes.

ANTI-MONEY LAUNDERING AUTHORITY (AMLA)

In 2025, representatives of the Lithuanian Financial Intelligence Unit actively participated in the activities of the Anti-Money Laundering Authority (AMLA) Board in its FIU configuration. Six meetings were held, during which various internal legal acts were adopted, including those regulating the selection, appointment, and working arrangements of FIU representatives at AMLA headquarters, as well as establishing AMLA's obligation to organise peer reviews of FIUs in order to promote the dissemination of best practices and strengthen operational effectiveness.

Representatives of the Lithuanian FIU actively participated in the activities of the Anti-Money Laundering Authority (AMLA) Board

EFIPPP GROUP

By decision of the Steering Group of the Europol Financial Intelligence Public Private Partnership (EFIPPP) initiative of the European Union Agency for Law Enforcement Cooperation (Europol), the membership of the Service and the Public Institution Money Laundering Prevention Competence Centre (hereinafter – the Public Institution Money Laundering Prevention Competence Centre) was approved in October 2021. The EFIPPP Group functions as an information-sharing platform, bringing together not only various law enforcement authorities, financial intelligence units, financial institutions, public-private partnership initiatives, and international organisations, but also uniting them across geographical boundaries. Participation in the activities of the EFIPPP Group ensures continuous engagement with the evolving landscape of anti-money laundering and counter-terrorist financing prevention.

In 2025, three plenary sessions of the EFIPPP Group were held, in which representatives of MLPB participated. Participation in the EFIPPP plenary sessions provides MLPB representatives with the opportunity to join various EFIPPP working groups dedicated to the analysis of specific financial crime typologies (e.g. fraud, money mules, terrorist financing, crypto-assets, child sexual exploitation, trafficking in human beings, and others), as well as to the exchange of information, experience, and insights at the cross-border level, including cooperation between the private and public sectors. Since 2024, a MLPB representative has been participating in a working group focused on child exploitation issues, the objective of which is to share national experiences and develop guidance for relevant stakeholders to identify financial transactions linked to child exploitation. In 2025, MLPB representatives additionally joined the working group addressing crypto-asset-related issues.

EMPACT CFMLAR GROUP

In 2025, MLPB representatives participated in six meetings of the European Multidisciplinary Platform Against Criminal Threats (EMPACT) CFMLAR Group (four in-person meetings and two virtual meetings).

OTHER MEETINGS (PROJECT-BASED ACTIVITIES)

In order to strengthen analytical capabilities and contribute to the implementation of international and European Union-level initiatives, MLPB also actively participated in various project-based activities, expert meetings, and inter-institutional initiatives.

Directorate-General for Structural Reform Support of the European Commission and Technical Support Instrument of the Council of Europe project "Preparation of a common baseline for an Anti-Money Laundering / Counter Financing of Terrorism Reporting system" (SMDS project). The objective of the project was to develop a Standardised Minimum Data Set (SMDS) to be used by obliged entities when submitting suspicious transaction reports (STRs) and transaction reports (TrRs) to FIUs across Member States. The SMDS aims to reflect a common understanding among FIUs and obliged entities regarding the meaning of specific terms, their reporting format, and interrelationships between data elements. The dataset could be applied by FIUs of all EU Member States and three EEA jurisdictions, thereby enhancing the efficiency of cross-border information exchange processes. Information on the requirements applicable to obliged entities when submitting STR, CTR, and VASP reports under the legislation of the Republic of Lithuania (including prescribed forms, required data, data submission formats, etc.) was systematised and provided to the project organisers. Information was also provided on the processes for the exchange of data with Financial Intelligence Units (FIUs) of other countries. The MLPB staff actively participated in project workshops by providing comments and proposals on the SMDS development.

11

METHODOLOGICAL SUPPORT

In 2025, MLPB staff actively provided methodological support and organised training sessions for financial institutions and other obliged entities. The Service continuously provided consultations on the interpretation of legal provisions and the application of the LPMLTF, examined inquiries from associations and other entities, and prepared and disseminated questionnaires and other methodological materials.

19 training courses were organized for non-financial sector entities.

In 2025, the scope of training and the number of participants significantly increased, with particular emphasis placed on non-financial sector entities. In total, 19 training sessions were organised for notaries, accountants, gambling and lottery operators, lawyers, auditors, and other obliged entities, with the aim of strengthening their capacity to properly implement anti-money laundering and counter-terrorist financing measures and to identify potential breaches. The training sessions covered anti-money laundering and counter-terrorist financing requirements, national and international risks, aspects of sanctions regulatory frameworks, the latest regulatory developments, as well as the most relevant typologies. The updated list of criteria for identifying suspicious monetary transactions or operations was also presented.

In total, 1,399 persons were trained in 2025, which is significantly higher than in 2024 (369 persons) and 2023 (763 persons). This increase demonstrates the growing engagement of obliged entities and the rising demand for methodological support. In addition, the MLPB allocates additional resources to the organisation and delivery of these trainings, ensuring effective knowledge transfer and methodological assistance to obliged entities.

In Q1 2025, two presentations of the National Risk Assessment were organised, both in-person and remotely via the YouTube platform (on the “Ekspertų slėnis” channel). The first presentation was dedicated to the payment services sector (approximately 50 participants in person and around 230 participants remotely), while the second was aimed at the VASP sector (approximately 50 participants in person and around 170 participants remotely).

In addition, the MLPB published an informational review on high-risk third countries and applicable requirements on the Service's official website. This review aimed to inform financial institutions, other obliged entities, supervisory and law enforcement authorities about applicable international lists, ensure compliance with legal requirements, and strengthen risk assessment and management practices by applying enhanced customer due diligence measures when dealing with clients or transactions linked to high-risk jurisdictions. The review also contributed to reducing money laundering and terrorist financing risks in Lithuania and strengthening the effectiveness of the national preventive framework.

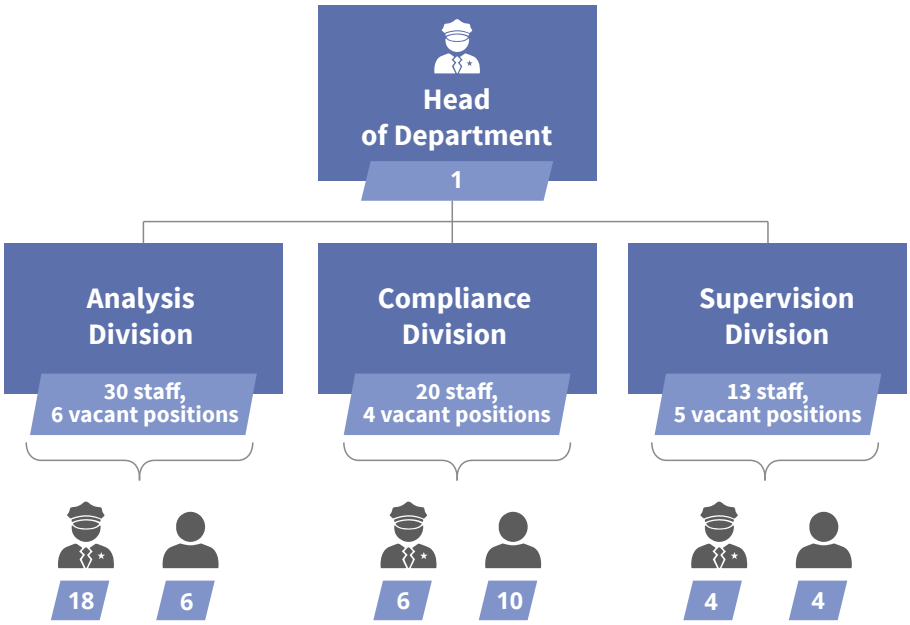
In summary, in 2025 the MLPB's methodological activities were characterised by increasing scope, broader engagement of obliged entities, and greater focus on the non-financial sector. The increased number of training sessions and participant engagement demonstrate a growing need to strengthen practical skills in the field of anti-money laundering and counter-terrorist financing. The methodological support provided and informational tools contributed to better application of legal requirements, improved understanding of risks, and overall strengthening of the effectiveness of the preventive system.

12

FINANCIAL INTELLIGENCE UNIT CAPACITIES

HUMAN RESOURCES

At the end of 2025, the MLPB consisted of three divisions (the Analysis Division, the Compliance Division, and the Supervision Division) and 64 staff positions, of which 29 were officers and 35 were other employees.



Financial resources

Year	Share of the Service's budget allocated to AML prevention	Additional budget allocated to improving the AML prevention system and supervisory solutions	Additional budget allocated to strengthening measures related to virtual assets
2021	727 000 euros	495 800 euros	300 000 euros
2022	1 388 511 euros	295 118 euros	-
2023	1 558 201 euros	-	-
2024	1 641 473 euros	135 00 euros	-
2025	1 831 334 euros	133 840 euros	-

13

OTHER INFORMATION

Statistical information

According to the Register of Suspected, Accused and Convicted Persons, in 2025, under Article 216 of the Criminal Code of the Republic of Lithuania (hereinafter – CC RL), four criminal cases were resolved by court judgments of conviction, resulting in 10 natural persons being convicted.

In 2025, 39 criminal offences were registered, 47 were investigated, 28 were discontinued, and 46 were referred to courts of first instance.

registered	investigated	discontinued	referred to courts of first instance
39	47	28	46

During 2025, 16 natural persons were registered as suspects of committing offences under Article 216 of the CC RL. The value of assets subject to temporary restriction of property rights amounted to EUR 3,366,414.

According to data from the Lithuanian Courts Information System (LITEKO), in 2025 the courts examined 14 cases concerning the laundering of money or assets obtained through criminal means.

No cases related to the financing or support of terrorist activities were examined by the courts in 2025.

Regulatory and supervisory authorities and number of staff responsible for the prevention of money laundering and terrorist financing

Regulatory and supervisory authorities	Number of staff working in the field of anti-money laundering and terrorist financing prevention
Bank of Lithuania	**19**
Department of Cultural Heritage under the Ministry of Culture of the Republic of Lithuania	**2**
Gaming Control Authority under the Ministry of Finance of the Republic of Lithuania	**5** positions
Lithuanian Bar Association	**6** (3 staff members of the Bar Association administration and 4 members of the Bar Council
Lithuanian Chamber of Notaries	**4**
Lithuanian Chamber of Auditors	**10** (1 administrative staff member and 9 members of the Quality Control Committee)
Chamber of Judicial Officers of Lithuania	**11** (5 regional representatives, 5 members of the Audit Commission, 1 staff member of the Chamber of Bailiffs administration)
Lithuanian Assay Office	**2**

FINANCIAL CRIME INVESTIGATION SERVICE

UNDER THE MINISTRY OF THE INTERIOR
OF THE REPUBLIC OF LITHUANIA

2026