LIETUVOS BANKAS
EUROSISTEMA

Overview of the ongoing monitoring of customers' business relationships and transactions

Analysis and Research

No 5 / 2023

Analysis and Research Series
No 5 / 2023

ISSN 2783-5944 (ONLINE)

Overview of the ongoing monitoring of customers' business relationships and transactions

The document was prepared by:
Financial Services and Market Supervision Department
Anti-Money Laundering Division
Contacts:
info@lb.lt
+370 800 50 500

Gedimino pr. 6, LT-01103 Vilnius
www.lb.lt

CONTENTS

Abbreviations and other explanations

EC	European Commission
EU	European Union
EEA	European Economic Area
EBA Risk Factor Guidelines	Guidelines from the European Banking Authority of 1 March 2021 after Articles 17 and 18(4) of Directive (EU) 2015/849 on customer due diligence and factors that credit and financial institutions should consider when assessing the money laundering and terrorist financing risk associated with individual business relationships and occasional transactions, repealing and amending Guideline JC/2017/37
FCIS	Financial Crimes Investigation Service under the Ministry of the Interior of the Republic of Lithuania.
FMP	Financial market participant
FATF	Financial Action Task Force on money laundering and terrorist financing
IT	Information technology
KYC	Customer due diligence information
Guidelines	The guidelines to FMPs aimed at preventing money laundering and/or terrorist financing, approved by the Resolution of the Board of the Bank of Lithuania No 03-17 of 12 February 2015 On the Approval of the Guidelines to Financial Market Participants Aimed at Preventing Money Laundering and/or Terrorist Financing
OEDD	Ongoing enhanced *due diligence* and monitoring process of high ML/TF risk groups during the course of business relationships
Operations	Payment operations and/or transactions
PEP	Politically exposed (vulnerable) persons
ML/TF	Money laundering and / or terrorist financing
ML	Money laundering
MLTFP	Prevention of Money Laundering and/or Terrorist Financing
Reports to the FCIS	Reports to the FCIS about suspicious monetary operations or transactions
AML/CTF Law	Republic of Lithuania Law on the Prevention of Money Laundering and Terrorist Financing
Monitoring	Ongoing monitoring of customer’s business relationships and operations/transactions
TF	Terrorist financing
SSD	State Security Department of the Republic of Lithuania

1. OBJECTIVE OF THE OVERVIEW

The Bank of Lithuania, in the course of its risk-based supervision, observes that FMPs face issues related to the practical implementation of monitoring. This document provides a brief overview of the purpose of the organisation and implementation of monitoring, the identification and interoperability of the monitoring model/framework and solutions, the adaptation of individual monitoring solutions, including monitoring scenarios, to the FMP's business model and the existing customer portfolio, as well as the periodic review and testing of the monitoring solutions, including automated scenarios. This review also aims to provide a brief overview of possible monitoring solutions in cases of increased ML/TF risks, best practices in the review of *alerts* generated by the automated monitoring system and in the process of conducting more in-depth internal investigations, as well as practical examples of internal investigations that have been carried out inappropriately.

The overview is based on the provisions of the legislation of the Republic of Lithuania, best practices of international organisations and other supervisory authorities, as well as best practices of financial institutions observed by the Bank of Lithuania in the exercise of its supervisory functions.

2. FRAMEWORK AND OBJECTIVE OF THE ORGANISATION AND IMPLEMENTATION OF MONITORING

Article 29(1)(3) of the AML/CTF Law states that FMPs must establish internal control procedures relating to the organisation of the monitoring of business relationships and/or transactions. Article 9(16) of the AML/CTF Law imposes an obligation on FMPs to perform ongoing monitoring of the customer's business relationships, including the investigation of transactions concluded in the course of such relationships, in order to ensure that the transactions are consistent with the FMP's knowledge of the customer, its business, risk profile and source of funds. Article 16(2) of the AML/CTF Law requires that if an FMP discovers that its customer is conducting a suspicious monetary operation or transaction, regardless of the amount of the monetary operation or transaction, the FMP shall suspend the monetary operation or transaction (unless it is objectively impossible to do so due to the nature of the monetary operation or transaction, the manner in which it was conducted, or any other circumstance), and report the monetary operation or transaction to the FCIS within 3 business hours of suspending the operation or transaction. Article 17(1) of the AML/CTF Law imposes an obligation on FMPs to pay attention to activities which by their nature may be related to ML/TF, and in particular to complex or unusually large transactions and any unusual transaction structures which do not have a clear economic or obvious legitimate purpose, business relationships or monetary transactions with customers from third countries where, according to information officially published by international intergovernmental organisations, the measures to prevent MF/TF are inadequate or do not meet international standards. Paragraph 2 of the same Article states that FMPs must investigate the basis and purpose of such transactions, document the results of the investigation in writing and decide whether to refer the suspicious transaction to the FCIS.

More details about the monitoring requirements applicable to FMPs are provided in Chapter VIII of the Guidelines (see other chapters for further details).

Paragraphs 4.72 to 4.75 of the EBA Risk Factors Guidelines state that FMPs should ensure that their approach to the monitoring of transactions is effective and appropriate. An effective transaction monitoring system is based on up-to-date customer information and should enable FMPs to reliably identify unusual and suspicious transactions and transactions with unusual structures. FMPs should ensure that their procedures are designed to review flagged transactions without delay. The appropriateness of monitoring procedures will depend on the nature, size and complexity of the FMP's activities and the ML/TF risk exposure of the FMPs. The EBA Risk Factors Guidelines state that FMPs should adjust the intensity and frequency of monitoring in line with the risk-based approach. In each case, FMPs should decide which transactions they will monitor in real time (online monitoring) and which transactions will be monitored *ex post* (retrospectively). FMPs have to decide whether they will monitor transactions manually or use an automated transaction monitoring system. It should be noted that FMPs with a high volume of operations should consider the introduction of an automated transaction monitoring system. As stated in paragraph 4.75 of the EBA Risk Factors Guidelines, in addition to real-time and ex-post monitoring of individual transactions, and irrespective of the level of automation applied, FMPs should regularly perform ex-post reviews of the entire sample of processed transactions to identify trends that could help to assess risk exposure, as well as test and – if necessary – subsequently improve the robustness and adequacy of their transaction monitoring systems.

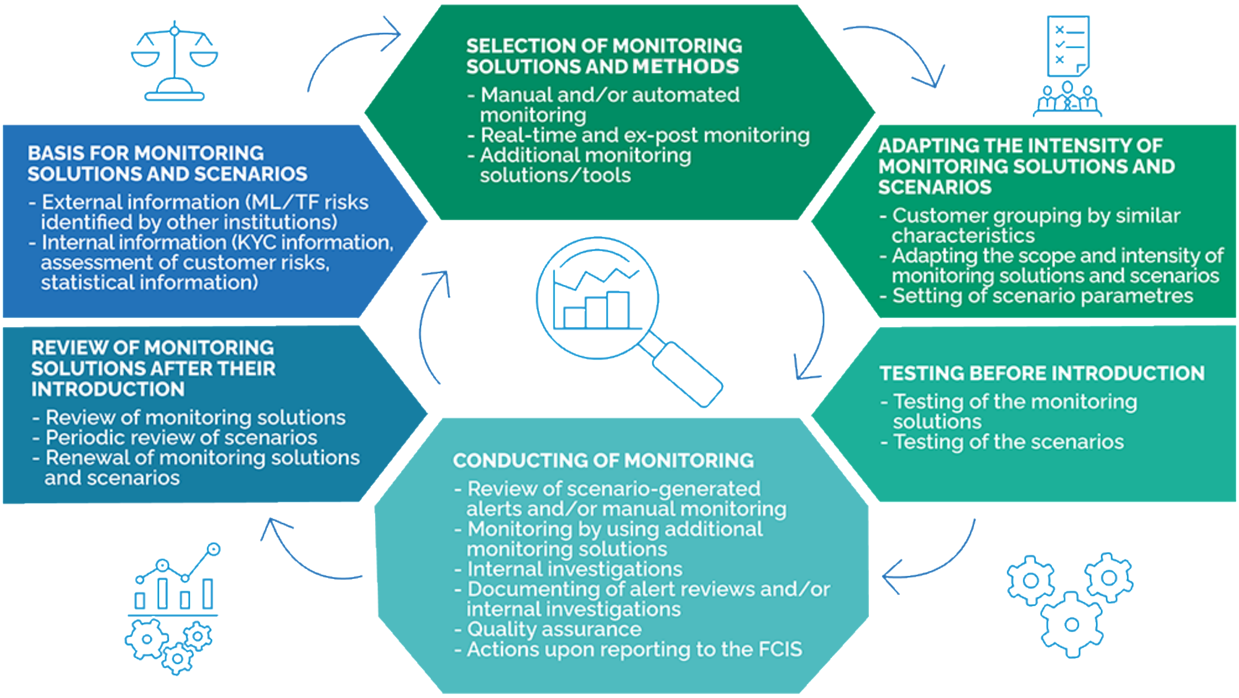
Firstly, it should be noted that the monitoring solutions, methods and the duties and mandatory actions to be carried out by FMP employees in the context of monitoring should be clearly regulated in the internal control policy of the FMP. Furthermore, when carried out in practice, the monitoring processes should be in line with the processes set out in the internal control policies of the FMP. For example, there should not be situations where an FMP develops a monitoring model in the light of various ML/TF risks and includes specific monitoring solutions and measures in its internal policies, but the monitoring solutions, as set out in the policies of the FMP are not applied due to lack of employees or other reasons.

It should be emphasised that FMPs should take a risk-based approach to monitoring. The risk-based approach means that FMPs must focus their attention and resources on those areas that pose the greatest ML/TF risk. When conducting monitoring, FMPs must be able to justify the chosen monitoring approach, the specific monitoring solutions and measures used.

A good, efficient and effective monitoring approach is based on optimal monitoring solutions, chosen according to the scale of the activities and business model of the FMP. The monitoring approach established by the FMP must be based on the FTP's knowledge of both the existing and the emerging risks of ML/TF, as well as on the FMP's good understanding of its customer base, which allows it to better identify unusual customer activity and to assess whether such customer activity could reasonably be considered suspicious. In order to have an effective monitoring approach, it is essential to establish a grouping of the FMP's customer portfolio that would serve as the framework for developing monitoring scenarios and implementing additional monitoring solutions, which should then be tested, continuously reviewed and updated.

The next equally important step is conducting monitoring in practice and the use of the information gathered during the monitoring process, not only to improve the FMP's understanding of its customer portfolio, but also to improve the monitoring approach and the solutions applied. Accordingly, it is concluded that all these processes are closely interlinked and must continuously complement each other (Fig. 1).

Fig. 1 Monitoring system cycle



SELECTION OF MONITORING SOLUTIONS AND METHODS
- Manual and/or automated monitoring
- Real-time and ex-post monitoring
- Additional monitoring solutions/tools
ADAPTING THE INTENSITY OF MONITORING SOLUTIONS AND SCENARIOS
- Customer grouping by similar characteristics
- Adapting the scope and intensity of monitoring solutions and scenarios
- Setting of scenario parametres
TESTING BEFORE INTRODUCTION
- Testing of the monitoring solutions
- Testing of the scenarios
CONDUCTING OF MONITORING
- Review of scenario-generated alerts and/or manual monitoring
- Monitoring by using additional monitoring solutions
- Internal investigations
- Documenting of alert reviews and/or internal investigations
- Quality assurance
- Actions upon reporting to the FCIS
REVIEW OF MONITORING SOLUTIONS AFTER THEIR INTRODUCTION
- Review of monitoring solutions
- Periodic review of scenarios
- Renewal of monitoring solutions and scenarios
BASIS FOR MONITORING SOLUTIONS AND SCENARIOS
- External information (ML/TF risks identified by other institutions)
- Internal information (KYC information, assessment of customer risks, statistical information)

It should be noted that the legislation does not impose a mandatory obligation on FMPs to apply automated monitoring. The approach and method of organising monitoring activities chosen by the FMP must be proportionate to the scale of the FMP’s business and its capacity to ensure appropriate management of ML/TF risks. In many cases, FMPs (with a larger scale of business and without sufficient capacity to review transactions by non-automated means) should evaluate the introduction of an automated monitoring system to generate alerts on unusual and/or suspicious transactions. In order to identify such transactions, FMPs should identify and understand the red *flags* of unusual and/or suspicious activity and incorporate them into the business *rules* scenarios used in the automated monitoring system. It should be noted that in the event that a FMP chooses to use purely manual monitoring solutions, it should also ensure that it has sufficient employees to carry out such monitoring, that it reviews transactions in a timely manner, that it carries out the review of transactions in a structured manner based on the rules chosen (e.g. defined criteria for transactions which are to be subjected to more detailed ex-post review), why it has chosen those particular rules and that it must periodically review and assess the effectiveness of such rules and criteria. It should also ensure both ex-post (analysis of transactions already executed) and real-time (before and/or during the execution of a customer transaction) monitoring.

3. BASIS FOR SELECTING AND SETTING UP MONITORING SOLUTIONS AND SCENARIOS

Requirements of the Guidelines
60. The FMP shall ensure that the process of monitoring the customer’s business relationships and/or transactions is organised taking into account the results of the FMP’s business-wide ML/TF risk assessment. This means that, having identified higher-risk areas (e.g. customers from high-risk countries, customers’ activities associated with a higher risk of ML/TF, a specific product offered by the FMP creates more favourable conditions for ML/TF), the FMP shall adjust the monitoring intensity, scope and scenarios and set relevant monitoring criteria to be able to ensure due and efficient detection and identification of suspicious transactions performed by the customer. 63. The FMP shall apply measures proportionate to the nature and size of business activity, ensuring effective ongoing monitoring of business relationships and transactions.

The requirement in the Guidelines stems from the fact that the business-wide ML/TF risk assessment process of an FMP should reflect all the ML/TF risks relevant to the specific FMP. Typically, the information used to carry out a business-wide ML/TF risk assessment includes both external and internal FMP information. The sources recommended as a basis for setting monitoring solutions and specific scenarios can be classified into two main groups: external and internal. First of all, the use of these sources must not be one-off exercise. On the contrary, the process of reviewing the monitoring solutions used by an FMP, including specific scenarios, and the assessment of the need to supplement or adjust the monitoring solutions as appropriate in order to effectively manage ML/TF risks, must be continuous and repetitive.

The following is a exemplary list of external and internal sources that a FMP should refer to when establishing its monitoring processes. This list is based on paragraphs 1.29 to 1.32 of the EBA Risk Factors Guidelines and best practice, but it should be noted that the list is not exhaustive (see Fig. 2).

Fig. 2 Exemplary list of external and internal sources

External sources	Internal sources of the FMP
• ML/TF risk assessment from the EC • Lithuanian national assessment of ML/TF risks • FCIS criteria for identifying suspicious monetary operations or transactions • FCIS Annual ML/TF Report • SSD National Security Threat Assessment • EBA guidelines and recommendations • FATF Recommendations and Alerts • Analysis of alerts or typologies issued by Interpol, Europol and/or local law enforcement authorities • Guidelines from international or other supervisory authorities, best practices • EU list of countries with a high risk of ML/TF • FATF list of high-risk countries	• Business-wide ML/TF risk assessment of the FMP • Emerging new risks • Changes in the customer portfolio or service offering • Information collected during FMP customer due diligence • Individual customer ML/TF risk assessment • Customer portfolio (by types of economic activity, other groups (segments) of customers) • Recommendations from internal or external audits • Results of employee quality assurance • Relevant statistical information on customer behaviour (transactions) • Knowledge and professional experience of the FMP • Results of analysis of completed internal investigations • Analysis of reports submitted to the FCIS

When selecting monitoring solutions/measures and defining monitoring scenarios, FMPs should foremost consider **external sources**.. The main external sources are the ML/TF Risk Assessment from the EC[1] (SNRA) and the 2020 National ML/TF Risk Assessment[2] (NRA). They identify and assess ML/TF risks at the level of the EU and the Republic of Lithuania. These ML/TF risk assessments identify the ML/TF risks specific to individual financial sectors (e.g. banks, credit unions, electronic money and payment institutions (EMIs and PIs), financial brokerage and management companies, etc.) and non-financial sectors (e.g. gambling, real estate, precious metals, trust company administrators, non-profit organisations, free trade zones, etc.). As regards ML/TF risks specific to non-financial sector, this is particularly relevant if the FMP serves customers from these sectors. For example, NRA 2020 highlights the lack of monitoring scenarios to detect terrorist financing; it states that some institutions in the EMI and PI sector do not carry out ex post monitoring; it also identifies various ML/TF risks related to fictitious services and shell corporations. It is also recommended that during the implementation of their monitoring solutions, including specific monitoring scenarios, FMPs take into account the FCIS criteria for identifying suspicious monetary transactions,[3] periodic warning from FCIS and annual reports from FCIS on the prevention of ML/TF activities,[4] which provide a more detailed description of the typologies in relation to money laundering and/or terrorist financing. The information provided in the annual National Security Threat Assessment Report from SSD is relevant when establishing the monitoring measures applied by FMPs.[5]

Looking at other external sources, it should be noted that FMPs that operate not only in Lithuania, but also in other countries, have customers residing outside of Lithuania and make cross-border and international payments, are exposed to global ML/TF risks, and it is therefore important to consider the reports published by international institutions, such as FATF, Interpol, periodically conducted *Serious and Organised Crime Threat Assessment (*SOCTA)[6] reports, the various typologies or alerts published by other countries (e.g. the UK Police, the *Joint Money Laundering Intelligence Taskforce JMLIT in the UK*, the *Financial Crimes Enforcement* Network (FinCEN) in the US); analyses and typologies published by *Egmont* Group[7] are also very useful. The analyses and reports published by the United Nations Office on Drugs and Crime (UNODC)[8] are also recommended for consideration.

All these external sources allow to take into account the geographical flow of the transactions, the countries of establishment or residence, nationalities of customers, region-specific typologies such as transit accounts, shell corporations, social engineering fraud, *money mules*.[9] It should be noted that, in line with the EBA Risk Factors Guidelines and FATF recommendations,[10] both real-time and ex-post transaction monitoring rules

[1] 2019 ML/TF Risk Assessment from the EC (*Report from the Commission to the European Parliament and the Council*)

(https://ec.europa.eu/info/sites/info/files/supranational_risk_assessment_of_the_money_laundering_and_terrorist_financing_risks_affecting_the_union_-_annex.pdf).

[2] 2020 National ML/TF Risk Assessment (http://www.fntt.lt/data/public/uploads/2020/05/final-nra_lt_v3.pdf).

[3] The list of criteria for identifying potential money laundering and suspicious monetary operations or transactions, approved by the Order No. V-240 of Director of the Financial Crime Investigation Service under the Ministry of the Interior of the Republic of Lithuania of 5 December 2014 On the adoption of the list of criteria for identifying potential money laundering and suspicious monetary operations or transactions(https://e-seimas.lrs.lt/portal/legalAct/lt/TAD/13a1a7307fef11e49386e711974443ff/asr).

[44] FCIS reports on the prevention of money laundering and terrorist financing (http://www.fntt.lt/lt/pinigu-plovimo-prevencija/veikla/ataskaitos/73).

[5] https://www.vsd.lt/gresmes/metiniai-gresmiu-vertinimai/

[6] https://www.europol.europa.eu/socta-report

[7] 2014 - 2020 case file analysis (https://egmontgroup.org/en/filedepot_download/1661/125), analysis of cases from 2011 to 2013(https://egmontgroup.org/en/filedepot_download/1661/33), analysis of 100 cases in 2015 with suspiciousness criteria(https://www.jfiu.gov.hk/info/doc/21-100casesgb.pdf).

[8] https://www.unodc.org/documents/money-laundering/Model_Provisions_Final.pdf.

[9] FCIS reports on the prevention of money laundering and terrorist financing (http://www.fntt.lt/lt/pinigu-plovimo-prevencija/veikla/ataskaitos/73).

[10] FATF Recommendations "Anti-Money Laundering and terrorist Financing Measures and Financial Inclusion"(http://www.fatf-gafi.org/media/fatf/content/images/Updated-2017-FATF-2013-Guidance.pdf).

should be reviewed and adjusted in the light of the EC (supra-national), national and the business-wide ML/TF risk assessment of the FMP and the observations made by the employees performing ML/TF prevention functions at the FMP. According to the 2018 report from the Council of Europe Committee of Experts on the Evaluation of the Anti-Money Laundering Measures and the Financing of Terrorism *(Moneyval)*[11] and the EC's risk assessment, the main risks that are important for the FMPs to focus on are cash transactions, non-resident operations, control of intermediaries, cross-border operations, fraud (including e-fraud), counterfeiting of documents, shell corporations, drug trafficking, tax evasion, smuggling, etc. According to UNODC information, the main typologies of offences observed are drug trafficking, arms trafficking, human trafficking, bribery and corruption, tax evasion, racketeering and cyber fraud. Likewise, the SOCTA assessment report indicates that around 80% of criminal groups operating in the EU are involved in drug trafficking, organised property crime, excise fraud (e.g. cigarette and alcohol production or smuggling), human trafficking, online and other fraud or illegal immigration (around 40% of which are related to the drug trade). The report is also useful for assessing the geographical risk posed by individual EU countries, as it describes routes for drugs entering the EU from Africa, the Middle East and Asia. It also lists the EU countries with the highest production of synthetic drugs, etc. The report also notes that certain typologies in Europe are expanding year by year (e.g. cocaine trafficking into the EU from Latin America, cybercrime, online child sexual exploitation, crimes related to waste disposal). The report notes that criminals take advantage of corruption (from the lowest to the highest levels of public administration). Around 80% of criminal groups use legal persons to launder money, around a half of criminal groups set up their own companies for money laundering purposes and according to statistics around 80% of international trade is conducted through direct payment transfers between customer accounts (i.e. without the need for the additional intermediation of credit institutions through the issuance of bank guarantees, letters of credit), therefore it is essential to improve knowledge of the typology of *trade-based money laundering* and to apply monitoring solutions accordingly. The same report points out that the money laundering techniques used by organised crime groups range from the simplest ones, e.g. investing in real estate or high-value commodities, to more sophisticated money laundering techniques, such as trade finance through the use of a large number of different companies (including shell corporations[12]), cash-dominated businesses, etc.

It is very important to underline that the information contained in these sources should not only be used to decide on monitoring measures, solutions or scenarios, but is also indispensable for internal investigations, for the development of internal instructions, guidelines, typology overviews, training materials for employees and for informing employees about the signs of suspicious activities.

When implementing their monitoring solutions/measures and new monitoring scenarios, FMPs should take into account **internal information, statistics and data** related to the specific FMP, such as the business model of the FMP, its customer portfolio, the nature of business of its customers, target customer groups and their specific features, the nature of payments, the countries of residence and the countries of nationality of its customers, the direction of payment transactions by foreign countries, the offering of services and products and service delivery channels. To identify the ML/TF risks of an institution helps a proper and thorough business-wide ML/TF risk assessment[13] (hereafter referred to as the "risk assessment"). A properly conducted risk assessment, as outlined above, is one of the key internal documents which provides the framework for deciding on the monitoring approach and the specific monitoring solutions and measures to be applied by the

[11] 2018 *Moneyval* Report "Anti-money laundering and counter-terrorist financing measures Lithuania"(https://www.fatf-gafi.org/media/fatf/documents/reports/mer-fsrb/Moneyval-Mutual-Evaluation-Report-Lithuania-2018.pdf).

[12] The Bank of Lithuania and FCIS Guidelines for Identifying Shell Corporations (https://www.fntt.lt/lt/pinigu-plovimo-prevencija/fiktyviu-imoniu-veiklos-pozymiu-nustatymo-gaires/4112).

[13] On 11 February 2021, the Bank of Lithuania published an overview on how to conduct a proper business-wide money laundering and terrorist financing risk assessment (https://www.lb.lt/en/publications/overview-of-business-wide-assessments-of-money-laundering-and-terrorist-financing-risks-performed-by-financial-market-participants).

FMP. Monitoring scenarios are developed and/or updated on the basis of the risk assessment and effective practical implementation of the scenarios is ensured, as appropriate.

In choosing their monitoring solutions, FMPs need to give additional consideration to new emerging risks, for example where certain global/regional events increase the risk of ML/TF (e.g. the first signs of the COVID-19 pandemic and associated factors, which led to an increased risk of fraud due to the non-receipt of goods, services, investment fraud etc., also the emergence of the crisis of migrants (from Belarus) or war refugees and potential risks, including additional sanctions against countries), or to certain changes in the customer portfolio or the service offering of the FMP (e.g. the introduction of new services to customers engaged in economic activities posing a higher ML/TF risk (e.g. virtual asset exchangers, brokers of derivatives *on the Forex* exchange market, gambling, etc.), or the introduction of services to a new geographic area with a particular type of ML/TF risk or criminal activity typology). In accordance with paragraph 38 of the Guidelines, FMPs are required to assess new emerging ML/TF risks and take additional measures to manage these risks as appropriate, including reviewing and/or updating the monitoring solutions and measures established by the FMP. FMPs should also take into account the updated EBA Risk Factors Guidelines, which focus on both the business-wide ML/TF risk assessment and the identification of new emerging risks.

In addition, it should be noted that a proper business-wide ML/TF risk assessment and the individual ML/TF risk assessment of a customer should start with an effective implementation of customer due diligence, i.e. the KYC principle. It is the proper and effective customer due diligence that is instrumental in understanding not only the ML/TF risks to the FMP, but also in better understanding the business of the customer as well as the nature of the business, and in identifying, through transaction monitoring, what may be considered as an unusual transaction by the customer, including in assessing whether the customer's behaviour may be considered suspicious. It should be noted that the collection of information about the customer should not be formalistic, as the information provided by the customer may be fictitious or misleading; it is therefore important to assess whether the information on the purpose and intended nature of a business relationship is consistent with the economic activities indicated by the customer and with the business and nature of transactions as indicated by other customers with a similar economic profile; in the event of inconsistencies or where there is a lack of clear economic rationale or logic, the customer should be approached for a clarification. Accordingly, during the course of the business relationship, this customer information must be kept up-to-date and compared with the actual business activities of the customer.

In particular, by properly identifying customers and collecting information on FMPs existing customers, FMPs could choose effective monitoring solutions/techniques and identify the relevant scenario parameters (amount of transactions, number of transactions, time period) above which certain customer transactions would be considered as unusual and may require more detailed internal investigations as well as requesting additional information or documentation from the customer to support the payment transactions. Therefore, when implementing and optimizing the monitoring model and individual solutions, including monitoring scenarios and their parameters, it is essential for FMPs to rely on the available statistical information on their customers, customer groups and customer segments (see Sections 4.1 and 4.2 for more details).

Finally, it is important to underline that where FMPs outsource the automatic monitoring system or any other monitoring solution/tool from service providers, i.e. third parties, the functionality of such monitoring tool (including the monitoring scenarios in the case of an automated monitoring system) should be tailored to the business model and customer base of the specific FMP; the FMP should control the functioning of such solutions and should be able to understand the ML/TF risks identified and managed by means of the monitoring solutions or specific scenarios, as the case may be, and be able to understand and explain whether the monitoring solutions are functioning correctly.

4. ADAPTING THE INTENSITY AND SCOPE OF MONITORING SOLUTIONS AND SCENARIOS TO THE BUSINESS MODEL OF THE FMP AND CUSTOMER ML/TF RISK PROFILE

Requirements of the Guidelines

58. The FMP shall conduct ongoing monitoring of the customer's business relationships and transactions. Ongoing monitoring of business relationships and transactions shall include both online monitoring, i.e. real-time monitoring of the customer's transactions, and retrospective monitoring, i.e. the analysis of the past transactions of the customer in order to understand the nature of the customer's transactions and/or to establish whether they are consistent with the FMP's knowledge of the customer and their risk profile and to identify any suspicious transactions performed.

61. The FMP shall set the intensity, scope and scenarios for monitoring the customer's business relationships and/or transactions and relevant monitoring criteria taking into account the results of both the business-wide and the individual ML/TF risk assessment.

62. The intensity, scope and scenarios for monitoring business relationships and transactions and relevant monitoring criteria shall be selected taking into account at least the following factors:

62.1 the type of the monitoring (retrospective, real-time);

62.2. the risk profile of the customer;

63.3. the risk profile of the geography or territory in which the business is carried out;

62.4. the risk profile of products and operations / transactions.

4.1. CHOICE OF MONITORING SOLUTIONS, MEASURES, NATURE, THEIR INTENSITY AND SCOPE

In order to determine the intensity and scope of monitoring, FMPs must first holistically assess and decide on the monitoring approach they plan to apply in the course of their business activities. The Guidelines require FMPs to carry out both online and ex-post monitoring, but it is up to FMPs to determine the extent of such monitoring, taking into account the ML/TF risk exposure and the business model of the FMPs.

As described in the previous sections, a proper business-wide ML/TF risk assessment of a FMP is essential for the proper establishment and adaptation of the monitoring toolkit in order for it to work effectively. Typically, the business-wide ML/TF risk assessment of a FMP involves classifying its customers into certain groups (e.g. natural and legal customers, classification by the ML/TF risk profile assigned to the customer, nature of the customer's business, etc.), while the ML/TF risk assessment of an individual customer and the scope of information collected and assessed during this assessment is relevant in order to group the customers during the business-wide ML/TF risk assessment. It should be noted that a proper business-wide ML/TF risk assessment gives FMPs a good understanding of their customer portfolio and its ML/TF risk profile. Following ML/TF risk assessments (business-wide and individual customer assessment), it is possible to move to the next stage and take measures to manage the different ML/TF risks posed by customers - in this case, to organise customer monitoring tailored to address specific ML/TF risks. One of the ways to properly implement this objective, as enshrined in paragraph 61 of the Guidelines, is the obligation for FMPs to determine the different intensity, scope, monitoring measures and scenarios of their monitoring solutions in the light of their ML/TF risk exposure.

The purpose of online monitoring is to prevent an initiated payment transaction from taking place, or to prevent the crediting of customer funds until the transaction has been analysed by the responsible employees of the FMP. It is understandable that FMPs with a larger business volume are unable to review every payment transaction, and therefore, as a general rule, online monitoring should be put in place to stop payment transactions that are likely to pose the highest ML/TF risk, in an effort to stop suspicious transactions and prevent criminal activity.

In the case of ex-post monitoring, customer payment transactions are not stopped before they are executed, but those that have already been executed over a certain period are reviewed and analysed based on certain parameters. The purpose of this monitoring approach is to gain a better understanding of the customer's longer-term business activities and to analyse the customer's transactions in more detail, to assess whether the customer's actual business is consistent with the activities declared by the customer to the FMP at the time of establishing the business relationship, consistent with the typical activities of economic activity of the sector in which the customer operates, or with the usual business activities of the customer at the time of establishing the business relationship. Depending on the business model of the FMP and the ML/TF risk posed by that business model, ex-post monitoring may be carried out either with the help of an automated monitoring system, or by manually selecting customer transactions based on certain criteria and analysing them; or an integrated combination of the two monitoring techniques can be used. It should be pointed out that when automated monitoring system alerts are reviewed ex-post, FMPs are advised to consider the possibility of reviewing customer transactions concluded over a longer period of time, instead of limiting themselves to the single specific transaction for which the alert was generated. Normally, it is only by assessing a customer's transactions over a longer period of time is possible to gain a better understanding of the customer and the nature of its business and, accordingly, unusual or suspicious customer activities and transactions can be identified. Furthermore, a review of a customer's payments over a longer period of time also helps to verify whether the monitoring solutions and scenarios applied by the FMP are working properly and efficiently (see Chapter 5 for more details).

As indicated in paragraph 4.75 of the EBA Risk Factors Guidelines, it should also be noted that in addition to the use of an automated online and ex-post monitoring system, by taking into consideration the FMP's business model, the scope and nature thereof, the customer portfolio of the FMP, the transactions performed by the FMP, its offered products and services and the complexity thereof, as well as other relevant circumstances, the FMP may apply further additional monitoring solutions and measures, in particular those of the ex-post kind, as a complement to the longer-term monitoring analysis /review (see below) of the customer's business activity (e.g. every 6 months, 1 year, or other frequency as set out in the internal control policies of the FMP), or additional technical monitoring solutions (e.g. customer website authentication, *blockchain* analysis tools etc.). It should be pointed out that the main automatic monitoring system may also have longer-term ex-post monitoring scenarios (e.g. 6 months), in which case it is recommended to harmonise these different monitoring approaches and, for example, when carrying out internal investigations to focus more on in-depth networks and links analysis, etc.

Additional monitoring measures and on their basis the more in-depth investigations of customer's activities and operations carried out can be instrumental in identifying weaknesses in the monitoring system applied by the FMP, while simultaneously helping to improve the FMP's monitoring system (its methods, techniques, organisation of monitoring), including individual monitoring scenarios.

In conclusion, it should be emphasised that the monitoring solutions, measures and techniques chosen by the FMP should complement each other and must be tailored to manage the ML/TF risks to the FMP in question. Below are some practical examples that FMPs can take into account when developing their monitoring solutions and/or monitoring scenarios:

Real-time monitoring could also be used in the following cases:

- the monitoring of transactions that are inconsistent with the risk appetite of the FMP (e.g. certain unacceptable countries, unacceptable specific customers (those with negative feedback), specific keywords (e.g. those related to certain activities (e.g. consulting services, virtual assets, etc.), sanctioned banks, etc);
- the monitoring of transactions of a large-value compared to other similar customers of the FMP;

- the use of scenarios and keywords to identify terrorist financing;
- to prevent situations where a customer seeks to avoid providing information or documentation in relation to higher risk transactions (transactions in large amounts that are inconsistent with the economic capacity of an average customer of the FMP, structuring of transactions, etc.);
- the use of other scenarios, focusing on the highest ML/TF threats as identified by the FMP;
- the use of other specific scenarios, such as transit accounts, dormant accounts scenarios (i.e. where accounts start to be actively used after having been dormant for an extended period of time). It should be noted that these scenarios with different parameters can also be used for ex-post monitoring;
- payments initiated from an IP address other than the one normally used by the customer;
- lists of international financial sanctions and other restrictive measures are monitored during online monitoring.

Retrospective monitoring could also be used in the following cases:

- where monitoring scenarios are complex, consist of several components and require more time to analyse the alerts they generate;
- where the aim is to identify deviations from the purpose and nature of using the services declared to the FMP, such as exceeding the turnover indicated in the customer questionnaire (in percentage terms or multiple times), payments outside the indicated geographical area or where the nature (purpose) of the payment transaction does not correspond to the customer's activity;
- scenarios to identify deviations from the normal activities of the customer;
- unusual and complex transaction structures (e.g. economically not viable);
- scenarios related to geographical risks (geographical risks specific to certain countries or regions, such as human trafficking, cross-border smuggling, drug trafficking, counterfeit goods, fraud, terrorist financing, etc.);
- scenarios involving customers with higher ML/TF risks, e.g. PEPs, virtual asset exchanges, brokers of derivatives in the *Forex* currency market;
- scenarios involving different products, such as cash transactions;
- additional terrorist financing scenarios;
- scenarios which help to identify *many-to-one* and *one-to-many* payment transactions, which in their nature are more effective for monitoring transactions of natural persons;
- when FMPs have sufficient human resources – a review of activities of customers with higher ML/TF risk in the course of one day, one week or other period set by the FMP.

Possible additional investigations, ex-post analyses and other tools:

- enhanced monitoring of business relationships of customers with a high risk of ML/TF (e.g. through OEDD actions) as a standard practice;
- where in *ad-hoc* cases a customer's ML/TF risk is identified as higher and additional monitoring measures are needed and review of certain customers is necessary;
- checking the links between associated customers (e.g. common counterparties, through common registration addresses, IP addresses, phone numbers, etc.);
- investigations into joint activities of big groups of customer companies;
- internal investigations into the activities of customers with particularly numerous and/or broad operations, with a view to identifying possible links between operations;
- internal investigations of individual customers when relevant information is obtained, e.g. when a supervisory authority declares that a potential customer is providing financial services without a licence or the necessary authorisation, it is necessary to check whether there have been any related operations through the FMP;

- investigations due to information that has become public (e.g. *Luanda Leaks, Panama Papers, Pandora Papers, Paradise Papers*, etc.);
- in case other adverse information about potential customers has emerged;
- using other measures to detect adverse media on a customer;
- in the event of requests for information from competent authorities, other financial institutions or the FMP's own other units reporting suspicious behaviour, activity or payments by a customer, etc.;
- in other cases where online or ex-post automated monitoring is not possible;
- additional specific technical monitoring tools (blockchain technology analysis tools, web page monitoring, etc.).

4.2. INTENSITY AND SCOPE OF MONITORING SCENARIOS

In terms of ways of adapting the intensity and scope of the automated monitoring scenarios, one of them is to group FMP customers into segments according to certain criteria. This grouping allows the FMP to create and understand the customers it serves, including the nature of a customer's business. With this information, monitoring scenarios can be better adapted to identify unusual or suspicious activity of a customer. However, it is important to emphasise that such customer grouping is most effective when the FMP has a larger number of customers with the same profile (e.g. by the ML/TF risk group assigned to the customer, economic activities the customer is engaged in, etc.) and a benchmarking exercise can be carried out in order to create a more accurate customer profile. If a deviation from the customer's usual activities is detected, the FMP may decide whether such operations are clear, or whether a more in-depth analysis and possibly additional information from the customer is needed.

The grouping of customers and/or products and services offered by the FMP is also important because, for example, a student (or a middle-income worker) and a high net worth individual belong to the same group of natural persons, but the number and/or value of operations performed by these customers may be significantly different as what is usual for a high net worth individual will be unusual or even suspicious for a student. It is important to note that even within the same ML/TF risk group, customers are characterised by different activities, therefore, the parameters of the monitoring scenario should be focused on what would be unusual for a particular group of customers. For example, while it may be normal for gambling companies to have frequent payments in small amounts and for the gambling company's customers to be connected from different countries (via IP addresses), this type of payment operations and behaviour may be completely unusual for a company operating in another business or natural person and may give rise to suspicions of increased money laundering risks. When adapting the scenarios, it is important to take into account all the products offered by the FMP (e.g. payments, deposits, trade finance, investments, foreign exchange, etc.), types of client identification, as this allows for the creation of a representative picture of the FMP's customer.

It should be pointed out that when adapting and developing their monitoring scenarios, FMPs should not always limit themselves to the setting of value (amount) and country (payment direction) alone, but they must consider the possibility of establishing more complex scenarios combining several scenario parameters, for example, the element of value and country of payment transactions; the element of the value of payment transactions and the PEP status of the customer; the element of the value of payment transactions, the legal form of the customer and the ML/TF risk category assigned to the customer.

Based on best practices, the FMP may take the following criteria into account when adapting the intensity of monitoring and scenarios, but this list is not exhaustive:

- General typologies (e.g. fraud) and their related scenarios and ML/TF risks may be relevant for the entire customer portfolio and not just to a particular group of customers, and on the contrary, certain typologies may be more specific to a particular group of customers (e.g. human trafficking);

- Individual ML/TF risk of a customer: scenarios with different parameters and/or thresholds may be defined according to the ML/TF risk group assigned to the customer;
- Customer types: natural persons (students, middle-income workers, high net worth individuals) and legal entities (micro-enterprises, medium-sized enterprises, large enterprises, non-profit organisations, etc.);
- Specific types of customer activities: payment services, virtual assets, gambling, other customers the activities of which must be licensed or authorised, etc;
- Cash-dominated economic activities of customers: monitoring and scenarios for cash transactions should be differentiated according to the customer's activity, whether it is cash-dominated (e.g. outdoor sales, food stops, etc.) or not (business services, wholesale, etc.);
- Services provided and products offered: instant and regular payments, private banking customers, local payments, international payments, cash transactions, remittances, trade finance, deposits, investment products, correspondent relationships, various other banking products;
- Geography: e.g. countries with high ML/TF risk appearing on FATF or EC lists, target territories, EU list of non-cooperative jurisdictions for tax purposes, customers associated with countries with higher TF risk. It is important to note that EEA countries are also classified at different levels of ML/TF risk, and therefore, when assessing the geographical risk, it is also important to take into account a country's level of corruption and crime, its characteristic typologies, cases where, for example, there is a big inflow of complaints or adverse media on customers established or residing in the country concerned, even though the country is not included in the FATF or the EC lists of non-cooperative countries and in similar lists. When assessing the geographic risk, attention should be paid to elements such as, for example, the citizenship of the customer or beneficial owner, the country of residence, the country of residence for tax return purposes, the location of the main economic activities carried out or even the country of activities of the major counterparties, the country of the IP address from which connection is made when identifying the customer or performing payment operations, etc).

It is essential to emphasise that, while the above criteria are easier to apply when an FMP defines the scenarios for automated monitoring, however, FMPs that carry out manual monitoring should also consider the possibility of incorporating similar criteria into their monitoring model (e.g. manual review of all customer operations performed to and from a particular high-risk country or target territory, etc., may be chosen as an additional monitoring tool).

4.3. SETTING PARAMETERS FOR MONITORING SCENARIOS

Once the segmentation has been performed in accordance with the various sample criteria set out above, the next step is to select the parameters and thresholds for the specific monitoring scenarios, usually by defining the time period for which the monitoring system will generate an alert (e.g., 1 day, 7 days, 1 month or more), and by defining the number of operations and/or the value that will trigger the system to generate an alert during the relevant time period. As mentioned above, respective parameters can also be adapted to the manual operation monitoring conducted by FMPs if no automated monitoring system is used.

When developing or deploying additional monitoring scenarios, it is essential to rely on the available statistical information on the FMP's customer portfolio and the operations performed by the customers, in order to better tailor, optimize and set the parameters and thresholds of the scenarios (the number, value of operations, etc) and the time period over which operations are carried out, i.e. the measure of time. In line with best practices, it is advisable to rely on statistical information specific to the relevant customer group/segment, as, for example, the size and number of operations of natural persons may be different from that of legal persons, and vice versa.

Scenario parameters can be chosen in different ways and methods: for example, by calculating using statistical or mathematical means the deviations from usual activities based on number and value of operations of specific group of customers (e.g. natural persons assigned to different ML/TF risk groups, e.g. low, medium, high), and by adapting the scenario parameters using expert judgment (e.g. the operations of high ML/TF risk customers may be of higher value, but FMPs, in order to monitor more of the activities of high ML/TF risk customers, may apply thresholds (e.g. number or value of operations) to the scenarios for high ML/TF risk customers that are lower than the average of the operations performed by such customers). It should be noted that whatever method of setting of parameters of the monitoring scenarios the FMP chooses, it is essential that the FMP is able to justify why the particular parameters and thresholds of the monitoring scenarios have been set and to understand what customer operations/activities they are intended to monitor.

It is equally important that, once the scenarios and their parameters have been set in the FMP systems, the FMPs should be able to change the scenario settings, parameters, thresholds and dynamics in a timely manner and at any time if they observe new typologies or suspicious customer activities. Therefore, the IT monitoring solutions used by FMPs should be flexible and FMPs should be able to quickly deploy additional monitoring tools when needed.

In order to properly set the parameters of the monitoring scenarios, it is important for FMPs to know which activities are common or usual for the customers or the respective customer segment and, on the contrary, which are less usual. If the scenario parameters and thresholds are set too high, operations will not be detected, analysed and reported to the FCIS accordingly; if they are set too low, a significant backlog of alerts to be reviewed may appear and the monitoring system will not be effective. However, the statistics available to the FMP on its customers and their operations should be assessed rationally and expert judgement should be used when modifying and updating the monitoring scenarios. This prevents situations where the available data does not accurately reflect the ML/TF risk exposure of the institution, e.g. in the cases where the institution has few customers or only has customers of high ML/TF risk assigned that carry out large-value operations, the average turnover of transactions may not be an appropriate measure, as transactions below the average may also be unusual or suspicious.

It should be pointed out that the development of scenarios and the choice of their parameters must avoid the manipulation or misuse of statistical information, as scenario parameters should be set on the basis of the emerging ML/TF risks rather than on the number of resources or the number of employees available to review and analyse all the alerts in a timely manner.

5. TESTING THE EFFECTIVENESS AND PROPER FUNCTIONING OF MONITORING SOLUTIONS AND SCENARIOS

Requirements of the Guidelines

65. FMPs must regularly review and back-test the solutions in place to ensure that they remain relevant and effective in the light of the institution's level of ML/TF risk exposure, as determined by the business-wide ML/TF risk assessment of the FMP.

69. The adequacy of internal controls for monitoring business relationships and transactions (including automated monitoring solutions, IT tools, etc.) must be regularly reviewed to ensure that the arrangements in place remain up-to-date and in line with the risk exposure of the FMP.

The Guidelines state that FMPs should regularly review their monitoring model (including both manual and automated monitoring solutions). Such a review should help FMPs to assess whether the monitoring solutions chosen and the specific scenarios for automated and manual monitoring cover all customer transactions, take into account the existing customer portfolio and the entire product and service offered by the FMP; it is therefore recommended:

1) to perform periodic reviews and holistic assessment of the entire monitoring model chosen by the FMP, the individual monitoring processes, solutions and IT tools used. It should be pointed out that FMPs should assess holistically all of their monitoring processes in place and their interoperability in order to assess the effectiveness of the monitoring model;

2) to perform periodic tests and improve the automated monitoring scenarios used in order to ensure that they are effective, relevant and targeted at elevated-risk operations and elevated-risk customer behaviour. It is important to note that such a review should not attempt to manipulate the test results and artificially reduce the number of alerts generated. It should be pointed out that if the customer portfolio of an FMP consists of a large number of customers with a high ML/TF risk exposure, the FMP needs to allocate sufficient resources, both in terms of human resources and IT resources;

3) where the solutions used by an FMP rely exclusively on manual monitoring, the effectiveness of such monitoring should be assessed, for example, by verifying whether the number of transactions is indeed such that automated monitoring solutions cannot be used, the effectiveness of the criteria for manual review of customer transactions should be assessed, etc.

Firstly, it is recommended that a holistic assessment of the FMP's system model and the solutions chosen examine the interoperability of individual monitoring solutions, and whether they allow for an effective and comprehensive monitoring of customers' business activities. Furthermore, it is recommended that FMPs assess whether their monitoring solutions cover at least the following key aspects (although it should be noted that the list is not exhaustive and that other aspects relevant to the specific FMP should be assessed):

- whether the scenarios and monitoring tools are based on SNRA, NRV and other relevant typologies, including where new typologies are introduced, and if the FMP has monitoring measures to identify such cases;
- whether the monitoring solutions and scenarios are tailored to the business model and the existing customer portfolio of the FMP (e.g. whether currency exchange operators have monitoring tools to identify related currency exchange transactions, whether financial institutions with complex customer structures apply integrated monitoring scenarios and additional monitoring solutions and tools, etc.);
- whether individual TF monitoring measures and scenarios beyond those designed to monitor the implementation of international sanctions are in place;
- whether monitoring measures are in place for all product specificities (e.g. trade finance, credit, investment products, etc.);

- whether all payment instruments (e.g. payment cards) are subject to monitoring scenarios;
- whether both incoming and outgoing payment transactions are monitored;
- whether fraud prevention scenarios or other monitoring measures are used;
- whether monitoring solutions are in place to identify when a customer deviates from its normal business activity or a typical business activity of a customer group engaged in similar economic activities;
- whether the monitoring covers the whole of the customer’s business activity, for example whether all customer’s accounts and conducted transactions are monitored by monitoring measures;
- whether monitoring measures for internal FMP operations are in place, i.e. in cases when both the payer and the payee are the customers of the FMP;
- whether the scenarios do not overlap;
- whether monitoring measures are in place to detect transit accounts, dormant accounts;
- whether online and ex-post automatic monitoring scenarios are technically working properly;
- whether during manual monitoring FMP assesses it’s rules on how transactions are selected for review;
- whether the alerts generated by monitoring scenarios are reviewed in a timely manner and whether the process of alert backlog is properly controlled;
- whether a process for reviewing and ensuring quality performance of monitoring solutions and scenarios is in place.

It is also recommended that in order to improve the monitoring scenarios already implemented by the FMP and its overall monitoring system model, the following best practices are taken into consideration during review and testing:

1) manual review of a sample of all transactions that are not subject to any scenarios or other monitoring solutions to ensure that such transactions do not include unusual or suspicious customer activity. For example, natural persons receive payments from a large number of persons, however, such activity is not subject to the automated monitoring scenarios designed to identify such activity, no additional ex-post monitoring measures are applied, also other automated monitoring alerts are only analysed by reviewing the single transaction for which the alert was generated, therefore it is likely that the FMP will not detect such customer activity with any of the used monitoring measures);

2) analysis of the findings of internal investigations carried out and periodically reviewing the reports submitted to the FCIS in order to assess whether the monitoring solutions and specific scenarios applied by the FMP are effective in detecting unusual or suspicious transactions;

3) assessment of information collected by other means (e.g. in the course of *ad-hoc* investigations during the process of updating customer information (etc., ongoing due diligence), in the course of analysis of transactions carried out over a longer-term by customers with a high risk profile of ML/TF, etc.) and identified unusual or suspicious customer transactions. The purpose of such testing is to assess whether the monitoring solutions chosen by the FMPs in detecting such cases having suspicious red flags are effective, and whether additional automated monitoring scenarios may need to be put in place or additional monitoring measures may need to be applied.

Secondly, as regards the review and testing of automated monitoring scenarios, the Bank of Lithuania, in its supervision of FMPs, observes that in practice the ways, methods and scope of assessing monitoring solutions, systems used by FMPs, including testing of monitoring scenarios, vary. Can be identified several aspects of best practices on how to test effectiveness of monitoring scenarios and the proper technical functioning of IT systems used for monitoring:

1) testing is carried regularly (e.g. once a year). Periodic testing consists in testing of the monitoring scenarios as such and of the technical functioning of the parameters applied therein (e.g. when testing, assessment is made whether there is any overlap between the alerts generated and applicable scenarios,

whether the generation of the alerts technically works without errors, whether the alerts are always technically generated in accordance with the parameters set in the IT systems, whether the parameters of the system and the scenarios continue to work properly and correctly after changes are made to the IT system and whether all operations are going through the scenario filter in monitoring system;

2) analysis of scenarios that generate a high number of false positives is performed with the aim to adjust these scenarios and their parameters in order to generate more accurate alerts;

3) the false-positive ratio is relied upon when testing scenarios and assessing their effectiveness, i.e. whether the alerts generated under monitoring scenarios result in internal investigations, and what is the proportion of such completed investigations;

4) assessment if it is necessary to have monitoring scenarios that do not generate any alerts at all;

5) in line with best practices, testing under statistical *above-the-line* (ATL) – *below-the-line* (BTL) methods is performed in order to assess the optimal parameters and thresholds of the scenarios, especially transaction value (amount) factor. Such tests are particularly effective in defining scenario parameters with the view of validating the relevance and effectiveness (efficiency) of the set parameters and thresholds. Under the said statistical methods, the parameters and thresholds of the scenarios (number of operations, values) are usually increased or decreased to achieve the most optimal values of the parameters, and in this way FMPs can reduce the number of the so-called false positives. Testing under the ATL approach consists in the review of system-generated alerts that exceed the parameters and thresholds set by FMPs, while the BTL approach is about reviewing alerts in the test environment, either by reducing the parameters and thresholds compared to applicable parameters and thresholds in the production environment or by reviewing and assessing operations that fall below the applicable parameters and thresholds set in the scenarios. Best practice suggests using both approaches, but it is particularly important to emphasize the BTL approach as it allows to ensure that the parameters and thresholds (e.g. value, number of transactions, time period) set with regard to the transactions carried out by FMP's customers are not too high (e.g. if, when reviewing transactions below the applied parameters and thresholds for the respective scenario, unusual or suspicious customer activity is observed, it means that the scenario parameters and thresholds have been set incorrectly (too high) and that the scenario parameters must be adjusted. It should be noted that this testing is most effective when customers are appropriately grouped into relevant segments (e.g. natural persons, legal persons, customers financial institutions, etc.);

6) sample testing and ex-post manual review of transactions that do not fall under the scope of monitoring because the scenario parameters and thresholds are below the ones set by FMPs (e.g. the following scenario is applied: seven or more customers send payments to one natural person in one day; the recommendation is to periodically review whether the threshold of seven or more customers is in line with the trend of transactions carried out by FMP customers or whether the thresholds set in the scenarios need to be lowered or raised).

Before introducing new monitoring scenarios, a FMP should test changes to the scenarios in a test environment. It should be noted that the test environment should be run on real data in order to properly optimize the monitoring system in accordance with the testing results. In addition, FMP should decide whether upon the introduction of new scenarios, testing should be carried out in a real environment in order to verify the effectiveness of the scenario update (in line with the FMP's objectives for which the scenarios were updated). Given that the parameters (number of transactions, value, time) set in the scenarios may change accordingly as the FMP's business model and customer portfolio change (e.g. by the customers' economic activity, their exposure to ML/TF risk, etc.), it is recommended that the parameters of the scenarios are reviewed and tested periodically. Best practice which should be noted is where the FMP ensures that all results of testing of new (recalibrated) scenarios and any subsequent adjustments are substantiated and respectively documented (documentation confirming that the scenario has been tested, is working properly and is effective).

Thirdly, as regards the manual monitoring of operations carried out by FMPs, it should be noted that most of the best practices referred to above are relevant and can also be applied to test the effectiveness of manual monitoring solutions.

It should also be noted that it is very important to familiarise the employees engaged in the monitoring function with the FMP's monitoring process, monitoring solutions and individual scenarios, to explain to the employees why the particular monitoring solutions or scenarios have been chosen, what risky activities of customers they are designed and aim to identify, etc. The purpose of such training is to make the employees conducting the monitoring function to consider whether the monitoring solutions or specific scenarios chosen by the FMP correctly detect unusual or suspicious activities. In this way, the employees could observe in practice that certain suspicious or unusual operations are not detected under any of the applicable scenarios, they could track new typologies and trends, and they should therefore be encouraged to suggest the introduction of new scenarios or additional monitoring solutions and techniques, and such suggestions should be properly documented. This would make the review, testing, optimization and improvement of the monitoring scenarios and the overall monitoring model used by the FMP a continuous and ongoing process.

FMP's employees should regularly inform the management of the results of assessment of the effectiveness of the monitoring systems in place, the main changes to the monitoring scenarios and the results of their testing. In cases where the testing of monitoring solutions and scenarios reveals that the monitoring solutions or specific scenarios used are not effective or not effective enough, the persons responsible for the implementation of the monitoring function (heads of the units, team leaders) should take action to address such weaknesses. Accordingly, the main findings of the testing of the whole set of monitoring measures and the need for changes should be communicated to senior management (e.g. the FMP's board member responsible for ML/TF).

In addition, it should be noted that where the FMP purchases its monitoring solutions (including the automated monitoring system) from third parties or outsources the monitoring function to a third party altogether, the FMP is not discharged from the obligation to periodically review and assess the monitoring solutions used in the FMP's operations as set out above.

In summary, the review and assessment of the FMP's monitoring solutions and processes helps to plan human resources, calculate the number of employees required, assess the effectiveness and necessity of the individual monitoring systems in use (which may lead to the introduction of new systems), evaluate the monitoring scenarios used and the overall effectiveness of the monitoring model applied by the FMP, as well as the areas to be improved.

6. ENHANCED ONGOING MONITORING OF BUSINESS RELATIONSHIPS WITH CUSTOMERS

6.1. ENHANCED MONITORING MEASURES AND THE IMPORTANCE OF THE OEDD PROCESS

Article 14(1) of the AML/CTF Law requires that FMPs carry out enhanced customer due diligence by applying additional measures of identification of the customer and of the beneficial owner where higher ML/TF risk is identified based on the risk assessment and management procedures established by the FMP, and in other cases set out in Article 14(1) of the AML/CTF Law. Under Article 14(5)(3) of the AML/CTF, one of the mandatory additional measures is the enhanced ongoing monitoring of the business relationship with customers who are identified as higher ML/TF risk in accordance with the risk assessment and management procedures set by the FMP.

The requirement for enhanced monitoring of the customer's business relationship can be implemented either by applying more stringent monitoring scenarios to of high ML/TF risk group customers or by taking other additional monitoring measures. In supervising the financial market, the Bank of Lithuania has observed that the best practice is the OEDD process applied by FMPs, which not only updates the KYC information of high risk of ML/TF customers at more frequent intervals, reviews and additionally verifies whether all the necessary information and documents have been collected from the customer in accordance with the internal policy procedures of the FMP, but also includes a more in-depth analysis of the customer's actual activities and transactions over a longer period of time (e.g. 6 months, 1 year). In this context, it should be noted that this process should not be considered as the main monitoring solution, however, it can effectively complement the set of monitoring solutions applied by the FMP as it is closely linked to the ex-post review of a customer's transactions.

It should be noted that an effective OEDD process is not possible without properly collected KYC information about the customer and a well-functioning system of the overall monitoring model. In line with best market practice, it is recommended that the OEDD process and its results be documented in a standard form, which could include, for example, the following information related to the activities and transactions of the customer:

- whether the customer's actual activities are consistent with those declared in the KYC questionnaire (e.g. whether type of activity carried out, turnover of transactions, payments, their direction/flow, purpose and basis and countries are consistent with the declared activities, whether transactions are carried out to the specified partners);
- whether the customer's transactions are consistent with the declared purpose of the account (e.g. if the client is financial institution, whether the customer's account is used to safeguard customer funds or also for it's customer payments);
- whether the customer deviates from his/her usual and typical past activities;
- whether the customer's transactions are clear and have a clear economic rationale;
- whether the payers or payees (including business partners) of the customer's transactions are understandable and consistent with the customer's declared activities;
- whether the source of the funds related to the transactions is clear;
- whether the customer performs any unusual or suspicious activities and/or transactions.

In addition to reviewing of transactions, it is also recommended to assess:

- whether the ownership and control structure of the customer (a legal person) and the nature of its business activities is clear;
- whether the customer's activities are subject to regulatory permits or other authorisations and whether such authorisations are valid;
- whether the source of the customer's funds and wealth is clear in general;
- whether there is no adverse media about the customer, the customer's representatives, beneficial owners and counterparties.

As part of this process, it is also recommended to further review and assess whether all the necessary information and documents have been previously collected from the customer, e. g.:

- whether the customer has provided all the documentation required under the FMP's procedures (e.g. evidence of verification of beneficial owners in reliable and independent sources);
- whether all the conditions that were set during the onboarding have been met (e.g. if such condition was set, obtaining from the customer the report on the performed AML/CTF audit within a reasonable period of time after the onboarding, etc.);
- whether the ML/TF risk group was properly assigned to the customer ;

- if the customer is subject to specific limits, whether such limits are properly implemented and complied with by the customer, in particular important in cases, when it is not possible to apply the limits by technical means alone and customer is asked to comply with set conditions (etc., not receive transactions from certain jurisdictions);
- the findings are documented.

The FMP has more historical data on old customers, and therefore, after a certain period of time from the onboarding of new customers, or after the start of the operations of such new customers, as additional measure all operations of high ML/TF risk customers may be reviewed to ensure that the activities are in line with the customer's declared or usual activities, that the customer's actual activities are similar to those of customers in the similar business sector, and that the customer's operations are not unusual or suspicious. The OEDD process can also be carried out some time after report to the FCIS about suspicious activities or operations of the customer was made, in order to ascertain whether the customer no longer engages in unusual or suspicious activities.

It is essential that the process of monitoring and collecting KYC complements each other, i.e. the information obtained during monitoring should be used to update KYC information, e.g. in the event that the customer's business has expanded (new business partners, geographic expansion of payments), which resulted in an increase in payment flows, in the event that the customer had declared that payments would be made only in the EU countries but they are made with third countries posing high ML/TF risk, etc. In this case, a risk-based approach is recommended, i.e. the more significant the changes observed during monitoring, the more important it is to update the customer information in the FMP's systems during monitoring and not only during the periodic review of customer information. If the changes are not significant, a FMP with numerous customers may have no technical capacity and sufficient human resources to take note of every deviation.

6.2. ONGOING ENHANCED MONITORING OF BUSINESS RELATIONSHIPS BETWEEN OTHER FINANCIAL INSTITUTIONS AND OBLIGED ENTITIES (CORRESPONDENT RELATIONSHIPS)

It is noted that FMPs usually classify customers that are other financial institutions (e.g. EMIs and PIs, companies providing various riskier investment services, various brokers, Forex companies, etc.) or other obliged entities (e.g. gambling and lottery companies or virtual currency exchange operators, etc.) to higher exposure to ML/TF risk according to the FMP's own procedures for assessing and managing the ML/TF risk.

However, before monitoring such customers, the first step is to properly identify the customer and understand the ML/TF risk posed by the customer. This process is indispensable for effective monitoring later. Such customers perform operations on behalf of their clients and often have correspondent relationships with them, and are considered respondents, and it is therefore important that such respondent customers would apply to their own customers appropriate procedures for identification of their customers and beneficiary owners, verification of the information obtained and proper monitoring.

Based on best practices, it is recommended that due regard is paid to the control measures applied by such respondent customers, by taking into account the business model, and that the following ML/TF risk factors and their scope are assessed (e.g. customers portfolio based on different criteria as only when understanding the customers portfolio the assessment may be properly be made as to whether the applied AML/CTF measures are proportionate). It is also recommended to properly document such assessments. Section 8.10 of the EBA Guidelines on Risk Factors generally provides, for all correspondent relationships, irrespective of the respondent's country of establishment, that FMPs acting as correspondents should consider, on a risk-sensitive basis, whether obtaining information about the respondent's major business, the types of customers it attracts, and the quality of its AML systems and controls (including publicly available information about any recent regulatory or criminal sanctions for AML failings) would be appropriate. In order to properly monitor and select the most effective monitoring tools, it is first important to properly consider the ML/TF risk posed by the respondent customer in terms of it's customer portfolio, products and services offered. Therefore, in cases of higher ML/TF risk, it is particularly recommended to take regard of the following risk factors:

- customer risks (types of customers served, types of their economic activity, PEPs, etc.);
- geographic risks (countries of residence and operation of customers, payment directions and jurisdictions served, high-risk jurisdictions, etc.);
- the services/products provided and the risks of the delivery channel.

Upon obtaining and assessing information on the ML/TF risk of a customer financial institution or other obliged entity, it is recommended to decide on the most appropriate monitoring solutions for that customer. In accordance with best practices and when FMP indicates higher ML/TF risk, the FMP is recommended to:

- in addition to the online and ex-post automated monitoring, review and analyse retrospectively customer's operations over a longer period of time to better understand the customer's activities and identify possible deviations from the declared activities;
- if customers have several types of accounts, such as a current account and an account for the payment to the customer's clients, the monitoring solutions can be tailored to individual account types to better conduct monitoring of the customer's activities;
- at the time of customer identification, the FMP should obtain, from the countries where the customer is established or where the customer plans to offer its services and carry out the authorised activities, copies of licences or authorisations required for the customer's activities, and verify whether the customer holds such authorisations, and also during the monitoring, the FMP should consider whether the customer's actual activities (e.g. payment flows, nature of activities) are consistent with those declared at the time of identification, and whether the customer is not carrying out activities in countries where it does not have the right to carry out the regulated activities concerned;
- adapt technical solutions to support the restriction or assessment of operations in order to check whether the customer is carrying out operations with countries where it is not authorised or licensed to provide services (to this end, the FMP should know the countries in which the customer is not operating and have them clearly recorded as it allows to compare customer's activity during monitoring; also, periodic ex-post reviews of the customer's operations may be carried out more frequently, especially for new customers);
- assess, in view of the ML/TF risk posed by the respondent customer's client portfolio, whether new restrictive measures should be applied or the existing ones should be modified e.g. prohibition of operations from/to certain countries via FMP accounts, prohibition of operations with certain groups of customers, limitation of operations up to a certain value, etc.;
- introduce restrictions that would enable a customer to carry out operations only upon providing additional documentation;
- in cases of high ML/TF risk, to apply enhanced monitoring measures to specific customers and to manually review all operations carried out by the customer or to obtain supporting documentation from the customer before carrying out operations;
- in cases of particularly high ML/TF risk, the FMP may consider the whitelist service provision, i.e. where the FMP only allows clearly specified customer activities, while non-specified activities are prohibited.

7. PREVENTION OF TERRORIST FINANCING

Requirements of the Guidelines

59. The FMP must have separate internal control procedures (scenarios) to detect:

59.1. cases of terrorist financing;

59.2. cases of money laundering.

First of all, it should be noted that according to the Guidelines, FMPs must have separate monitoring solutions and/or scenarios to detect TF cases, but in practice it is often observed that FMPs do not have such scenarios or associate the monitoring of TF cases with the scenarios intended for the control of international sanctions or other restrictive measures.

As regards TF, it should be noted that terrorists use similar schemes as money launderers in order to evade the attention of law enforcement authorities and to conceal the identities of their financing providers, the source of funds and the identities of ultimate beneficiaries. It should be noted that the funds intended for TF can come from legitimate activities (e.g. non-profit organisations, donors, employees salaries, etc.) or from criminal acts, such as kidnapping ransoms, drug trafficking[14], arms trafficking. As for TF-intended funds from legitimate activities, the risk is particularly high in cases of local extremism which often do not require a lot of funds to carry out terrorist acts. Furthermore, the determination of funds derived from legitimate activities as related to TF is more complicated and may often require the use of more investigative tools, such as additional searches for adverse media about the customer where the customer publicly expresses support for the activities of terrorist organisations, etc.

It should also be noted that some sources suggest that terrorist financing should be defined by the broader term "*resourcing*" as the sources of TF may be not only remittances of funds but also shipments of goods (e.g. electronic goods) and the proceeds of such goods can be used to finance terrorist acts. Various trade-based money laundering schemes (e.g. *over-invoicing, under-invoicing, ghost-shipping,* etc.) can also be used for TF.

The TF risk is often associated with certain higher-risk countries, therefore, it is not only the countries as such but also individual cities or regions where the TF risk is elevated that should be considered (e.g. Turkish-Syrian border cities such as Gaziantep, Mardin, Sanliurfa, etc.). When assessing the geographical risk, it is important to not focus solely on the best-known terrorist organisations such as ISIS but to look at the TF risk in the African region, the North Caucasus, South-East Asia and etc.[15] For this purpose, it is recommended to also look at the country risk indexes published by Transparency International and human rights organisations as terrorist organisations often tend to operate in countries with high levels of corruption, human rights violations, etc.

Accordingly, when conducting investigations, it is important to focus not only on the usual terrorist organisations such as Al-Qaida, ISIS and Boko Haram, but also on radical right-wing groups (domestic terror),

[14] https://www.state.gov/2020-international-narcotics-control-strategy-report

[15] https://cisac.fsi.stanford.edu/mappingmilitants#highlight_text_11651; https://www.state.gov/country-reports-on-terrorism/#crt; https://reliefweb.int/sites/reliefweb.int/files/resources/GTI-2022-web.pdf

which risk is increasing.[16] It should be noted that the typologies specific to terrorist financing are detailed in both the National Threat Assessment[17] and the FATF Guidelines.[18]

In terms of TF prevention and customer monitoring, it is important to have not only appropriate monitoring solutions and/or scenarios in place, but also to carry out high-quality internal investigations addressing the various TF risk factors, i.e. when developing TF scenarios, in addition to geographical risk factors, the FMP should also consider the activities that may provide funding, such as drug trafficking (example Afghanistan and the opium and heroin trade route).

The following factors should be taken into account in TF-related scenarios, but it should be stressed that this list is only indicative and should not be considered as a minimum or exhaustive list:

- cash deposits followed by operations to conflict zones (natural persons, non-profit organisations);
- the value of the customer’s income and payments does not correspond to the customer’s declared employment activities;
- payments made on behalf of third parties in order to disguise the real payer or payee;
- the account is used to collect funds and then transfer them to countries with higher ML/TF risk;
- payments made to countries that are not related to the customer’s usual or economically explainable business;
- connections from IP addresses located in conflict zones or countries with high TF risk;
- payments to and from conflict zones and cash withdrawals in conflict zones;
- payments to charitable organisations located in Syria and other conflict zones or adjacent countries;
- the customer’s financial activities related to travel to conflict zones, such as buying plane tickets to Syria via Turkey and other points of entry, including Jordan, Lebanon or Israel;
- using of virtual assets to gain a degree of anonymity;
- complex scenarios that also look at the overall picture of the customer, i.e. not only the countries to or from which the customer sends or receives payments separately, but also looking at the flow of all payments.

Additional information on practical TF activities and the latest typologies is often reflected in various public reports and studies, such as those of Europol, RUSI Institute.[19]

[16] https://www.theguardian.com/us-news/2021/sep/08/post-911-domestic-terror

[17] National Threat Assessment, 2019 (https://www.vsd.lt/wp-content/uploads/2019/02/2019-Gresmes-internetui-EN.pdf).

[18] Terrorist Financing Risk Assessment Guidance, 2019 (https://rm.coe.int/terrorist-financing-risk-assessment-guidance-fatf/16809676a3, https://www.fatf-gafi.org/media/fatf/documents/reports/Financing-of-the-terrorist-organisation-ISIL.pdf; https://www.fatf-gafi.org/publications/methodsandtrends/documents/tf-west-africa.html).

[19] https://www.europarl.europa.eu/RegData/etudes/BRIE/2021/659446/EPRS_BRI(2021)659446_EN.pdf; https://rusi.org/explore-our-research/topics/terrorist-financing

8. INTERNAL INVESTIGATIONS

Requirements of the Guidelines

66. When monitoring the customer's business relationships and transactions, the FMP shall ensure that every alert generated by an automated monitoring solution (where the FMP has automated monitoring solutions in place) or every transaction of the customer (where the FMP does not have automated monitoring solutions in place) matching criteria of suspiciousness is duly reviewed and properly analysed by the FMP's employees and such actions are documented and stored in a format that makes it possible to present them to the supervisory authority

67. Where it is determined during the FMP's process of monitoring of business relationships and transactions that the activities of a customer (s) are subject to an internal investigation, the results and conclusions of the internal investigation must be documented, by clearly describing the course and outcome of the internal investigation, including the basis on which the relevant decision was taken (decision to terminate or extend the scope of the internal investigation or to report to the FCIS on the identified suspicious operations, etc.), and must be retained for the time set out in the AML/CTF Law.

First of all, it should be noted that, although the legislation does not define the definition of an internal investigation, in practice it is observed that an investigation is normally considered as a more detailed analysis requiring additional action by the FMP's employees, rather than simply a routine review of an alert generated by the monitoring system and its closure. Thus, it is up to the FMPs to define the concept of an investigation and the actions to be carried out in the course of an investigation, but the emphasis is the end result which means that both the analysis of the alerts generated by the monitoring system and the more in-depth investigations should not be carried out formally. When reviewing the alerts generated by the monitoring system or conducting more in-depth investigations, both the information previously provided by the customer and new information obtained from the customer, as well as the following aspects should be critically evaluated (but it should be noted that this list is not exhaustive):

- the rationale, logic and economic justification of payment transactions;
- an overall assessment of whether the customer's actual activities are in line with the customer's declared activities or activities typical of customers operating in the same business sector;
- assessment whether changes in the customer's activities (e.g. changes in payment directions, flows, countries, new partners) can be reasonably explained;
- assessment of the source of the funds involved in the transactions, directions and flows of payments and the basis for the payments (e.g. Saudi Arabia, the world's largest oil producer, is unlikely to import petroleum products, or Brazil is unlikely to import oranges, as it is the world's largest orange producer);
- assessment whether payments made by the customer in respect of goods or services are in accordance with the nature of the customer's declared business;
- assessment of the value of operations (e.g. the value is not in line with the value of the economic activities declared by the customer or with the value of transactions that are normal for a similar business sector);
- assessment of cases where operations are excessively complex and the customer does not provide a reasonable explanation for such complexity, or where operations are conducted with counterparties in the target territories and the customer cannot provide a reasonable explanation for the transfer of funds through companies established in the target territories;

- careful consideration is given to information from public sources, both about the customer and its counterparties with whom operations are conducted.

Best practice observed is when suspicious counterparties of one customer are identified for possible ML or TF, the FMP conducts a broader internal investigation and searches the database of transactions of all customers to see if more FMPs customers have conducted operations with such counterparties and, if such transactions are identified, takes action to manage the ML/TF risk. It should be noted that the result of internal investigations (e.g. an employee's findings on a customer's transactions or activities, the basis for a decision (e.g. a decision to terminate or extend the internal investigation, or to report suspicious operations to the FCIS, etc.), etc.) should be clearly documented. In addition to the results of the more in-depth investigations carried out, the results of the review and analysis of the alert generated by the monitoring system should also be documented.

8.1. DETERMINING THE IMPORTANCE OF REVIEWING OF ALERTS

FMPs with a larger scale of operations, more different monitoring scenarios used and more employees that perform the monitoring function may choose to prioritise review of alerts based on different risks and to delegate the analysis of the "riskiest" alerts to employees who are more experienced.

The prioritisation of alerts review should be consistent with the application of a risk-based approach, which means that the customer's activities posing the greatest ML/TF risk should be reviewed first. When implementing automatic monitoring scenarios, the priority of alert review can be set accordingly (e.g. low, medium, high). The FMP should arrange its monitoring in such a way that alerts are reviewed in accordance with the FMP's internal time frames and that a backlog of alerts does not occur, however, if a backlog occurs the priority is given to review of earlier generated alerts. Furthermore, it is recommended that the alerts generated by the monitoring system of the FMP are reviewed based on the ML/TF risk category of the customer (e.g. where the customer is a PEP, the alert generated by the system for monitoring his/her operations will be prioritised) and the risk level of the scenario (e.g. TF scenarios will have a higher priority than ML scenarios, etc).

8.2. TIMEFRAMES FOR INTERNAL INVESTIGATION

The legislation does not set a specific timeframe within which a review of the alerts generated by the monitoring system or a more in-depth internal investigation must be carried out. It should be emphasised that the very purpose of the prevention of ML/TF is the prevention of criminal activity, which is why the review of alerts or investigations into suspicious activity of a customer must be carried out as quickly as possible. Where investigations are initiated but not necessarily completed within a reasonable period of time from the date the alert is generated, there is a risk that effective prevention of ML/TF will not be ensured in terms of the timely identification of suspicious monetary operations and reporting to the FCIS.

8.3. DOCUMENTING INTERNAL INVESTIGATIONS

As also stated in the Guidelines, the audit trail of alert reviews and internal investigations should be visible and clearly documented from the moment an alert is generated in the monitoring system or the start of an internal investigation based on another reasons. When properly implemented, this process should make it clear which employees, when and on what basis carried out the investigation that was opened, and what conclusions of the investigation and on what basis they were made.

This audit trail documentation should be done automatically with the help of the IT system, to minimise the intervention of an employee in the process and to avoid that he/she deliberately skips certain steps.

The documentation of the investigation as such must be clear, based on facts/information substantiating as to who, when, where, how and why conducted the operations (or a single operation). Both the period of time over which payment transactions were reviewed and the conclusions as to why the customer's activity is or is not unusual or suspicious must be clearly stated, as well as the rationale for the decisions taken (e.g. to discontinue internal investigation). For more ideas on the content of the documentation of investigations, it is also recommended to take note of the FCIS's Memorandum on Reporting Suspicious Monetary Operations.[20]

For consistency purposes, it is recommended that the financial institution would have a single template or principal guideline for documenting investigations, regardless of which employee conducts the investigation. It should be noted that, in order to ensure consistency of investigation documenting as such, it is recommended, in line with best practices, that the most important "fields" should be mandatory, without which the investigation could not be completed.

A well-documented investigation is not only important for the assessment of a customer's activities at a specific time, but also for future investigations to be performed by the same or different employee, therefore, it is important that the conclusion of the investigation is clear and that it is possible to compare the customer's current activities with the previous ones.

8.4. ENSURING THE QUALITY OF MONITORING CONDUCTED BY EMPLOYEES

In order to continuously improve the monitoring activities, to monitor whether employees follow the established procedures in practice and to ensure a proper monitoring process, it is recommended to carry out a quality assurance check of the work carried out by individual employees engaged in the monitoring process.

For quality assurance checks, it is recommended to use a standardised form to record the results of the check. In addition, an FMP may establish, in a separate procedure, a methodology for calculating the quality assurance check results and set key performance indicators at which employees would be deemed to have achieved acceptable or unacceptable quality results.

It is recommended that quality assurance checks are carried out periodically (e.g. monthly or every few months) and that the results of the checks are communicated to employees, and that training is provided to the relevant function in the event of recurrent errors.

At the same time, it is recommended that the FMP applies a risk-based approach to the scope of the quality assurance checks to be carried out, e.g. more frequent and more extensive quality assurance checks (e.g. reviewing a larger sample of customer files) for new employees, when a certain FMPs internal process is amended or a new one is put in place, when a new IT system is put into operation, when an internal ML/TF audit or external review identifies a specific weaknesses in an area that needs improvement to ensure that the weaknesses are not recurrent, etc.

8.5. ACTION FOLLOWING A REPORT TO THE FCIS

Where an FMP notifies the FCIS of a suspicious activity or operation of a customer and decides to continue its business relationship with the customer, it should be noted that the previous reporting to the FCIS does not relieve the FMP of its obligation to continue to monitor such a customer, in particular if the customer's activities have been found to be suspicious or attributes of unusual activities have been determined, which

[20] https://www.fntt.lt/lt/naujienos/parengta-pranesimu-apie-itartinas-pinigines-operacijas-ar-sandorius-atmintine/4137

implies that such customers pose a higher ML/TF risk. In the case of such customers, monitoring may be enhanced, for example, by conducting more detailed reviews of the customer's activities at certain intervals set, manual review of each operation, CEO's approval of operations, and an assessment whether or not the customer continues the operations reported to the FCIS. However, it should be noted that the FMP, in carrying out such enhanced monitoring, has to ensure, as required by law, that the customer is not aware that its activities have already been reported to the FCIS.

8.6. EXAMPLES OF INADEQUATE MONITORING

Examples where monitoring and investigations have been deficient are presented below. The most common errors are those where, although operations were detected through FMP monitoring tools, investigations were carried out formally, the full picture of the customer's activities was not considered, the customer's activities and the source of the funds was not sufficiently ascertained, activities bearing suspicious attributes were not sufficiently assessed and therefore sufficient information and documentation substantiating the customer's activities was not collected.

Example 1

Customer A is a natural person with a payment operation turnover of approximately EUR 1 million over several years. Within seven calendar days, the customer received four payment totalling EUR 205,000 from his/her personal account in Qatar to his/her account opened with the FMP. It is stated in the KYC questionnaire that the customer is a Ukrainian citizen working as a lawyer in Lithuania with a gross salary of EUR 800. The customer's account statement for the past year shows that such large payment transactions are not typical to the customer and the FMP had no knowledge of the customer's other sources of funds. The FMP suspended the transactions and found out that the purpose of the funds received was the purchase of real estate. The FMP stated that the funds were received from the sale of a car owned by the customer (contract attached). The FMP did not carry out any additional investigation into the documentation on the source of the funds, in particular with regard to the discrepancy between the salary and the value of the car sold, nor did it carry out any additional investigation.

Example 2

Customer B's payment operation turnover is approx. EUR 4 million per year. During the onboarding, the customer stated in the KYC questionnaire that the account with the FMP would be used to receive income from the company's activities and to make payments related to its major business, with the company's main counterparties identified as companies engaged in pharmaceutical activities and the expected average monthly turnover was declared up to EUR 150,000. The customer's first operations in the account were as follows: on 25 May, EUR 700,000 was received from Company X and sent to Company Y within an hour, EUR 500,000 was received from Company Z and sent to Company Y within an hour, on 26 May of the same year, EUR 200,000 was received from Company Z, EUR 200,000 from Company X and EUR 400,000 sent to Company Y within an hour. The said operations did not correspond to the activities declared by the customer in the KYC questionnaire and there had been no prior payments on the account, but the FMP failed to consider these operations as transactions of an unusual size and structure, especially in view of to the fact that the funds received were immediately transferred, which refers to the characteristics of a transit account.

Example 3

Customer C is classified as high risk for ML/TF. The customer's place of registration is the Free Economic Zone of Northern Cyprus and its legal status is that of a legal person. Over the year, the customer carried out 520 operations worth around EUR 120 million, the majority of which were analysed after alerts were generated in the monitoring system. The customer's declared activity is the supply of IT equipment and services to business customers, with several business partners indicated. The contract with Partner X stipulates that Customer C will provide acquiring services, but in practice the nature and amount of the payments made do not correspond to the contractual terms. Customer C's only revenues to the account (EUR 60 million received in the customer's account) are received from a virtual asset exchange platform. The purpose of the incoming payments is the exchange of virtual assets into euros. The purpose of such payments does not relate to the customer's information held by the FMP and the nature of the customer's business. It should be noted that the FMP employees analysed a large part of the payments, but in all cases the only finding was that the virtual asset exchange platform was a known virtual asset exchange and therefore no further issues were raised, no further action was taken, even though the nature of the payments did not correspond to the information about the customer held by the FMP.

Example 4

Customer D's turnover since the start of the business relationship, i.e. over a period of two years, amounts to approximately EUR 1,80 million. The Customer is a natural person who is linked to an FMP employee who carried out the analysis of this customer's payments. The findings of the analysis are the same as the information provided in the field of the purpose of the payment, which was "gift", "same recipient", etc. The customer made 95 payments with the value of more than EUR 150,000 to various natural and legal persons with the purpose of the payments being "charity, donation", but no information on these payments is provided in the file. The customer also made a one-off transfer of EUR 250,000 to a beneficiary, but the conclusion of the monitoring officer, upon completion of the analysis of this payment, was "same beneficiary" and no additional documents were collected.

Example 5

Customer D's turnover since the start of the business relationship, i.e. over a period of two years, amounts to approximately EUR 1,40 million. The Customer is a financial institution that uses the services of the FMP to make its customer payments. According to the information provided by the FMP, almost all of the funds entering the customer's account consisted of funds transferred by Company A, amounting to approximately EUR 60 million. Although based on information received from FMP almost all the operations were automatically suspended, however, all these operations were marked with the same non-exhaustive general comment: "same beneficiary". No other comments are made on the source of the funds, the nature of the operations, their reasonableness, etc. According to the commercial register data, Company A has not been active since 2012 and the beneficial owners of Customer E and Company A are the same. The FMP indicated that the transactions were between two financial institutions but failed to provide additional documentation or further explanation.

Example 6

Customer F and Customer G have the legal status of a legal person. The business relationships with the customers were established at a similar time, with turnover since the beginning of the business relationship, i.e. within half a year, amounting to around EUR 25 million and EUR 18 million respectively. Although the representative of both customers is the same person, the beneficial owners are different and the customers' business model is similar. Both customers are engaged in e-commerce and, although they sell different products, each of them has several websites with very similar designs and the products sold and even the layout of the websites are identical. The operations and activities conducted in the accounts of the two customers are very similar, with almost all incoming funds being payments for goods sold and almost all outgoing funds being payments for IT, marketing or consultancy services. The two companies both receive funds from the same senders and send funds to the same beneficiaries. It should be noted that, according to their identical contracts with Company B, both customers purchase website and mobile app development and installation services from Company B, but, according to the information on Company B's website, Company B operates in the field of payment services, and does not offer the services referred to in the contracts with customers F and G. It should be pointed out that, although Customer F and Customer G are companies that were set up less than a year ago, they have received very large sums of money from the sale of their goods over the six months they have been operating. Given the date of establishment of both companies, the nature and size of their activities (according to publicly available information, each of the companies employ only one person), both the amounts for goods sold and the amounts for services purchased are unreasonably high.

Example 7

The activities stated by Client H are virtual asset exchange and derivative investment provider, with a legal status of a legal person. The customer's place of registration is Cyprus and the licence to operate is also issued in Cyprus. The customer's questionnaire features that it provides services in all EU countries except Hungary, Poland, Latvia, Spain, Belgium, Germany, and France (notably, these are the countries where the customer is not licensed to provide services). The value of payments made by the customer is around EUR 30 million, and most of the payments were analysed by the FMP's monitoring employees. For example, the customer received 10 payments from a customer who is a natural person in France, with the total value of EUR 70 000, and for such payments, the FMP states that the customer's activities are consistent with the declared ones. However, when analysing the customer's payments, the FMP failed to consider the information provided in the customer questionnaire regarding the countries where the customer is not authorised to provide services. In terms of the customer's activities in general, almost 20% of operations came from countries where the customer has no plans to or cannot conduct activities. It should be noted that around 80% of the complaints received about a customer's activities come from clients in countries where FMPS stated that it does not provide services. The client complaints contain, inter alia, additional information that the customer uses more websites than it had reported during the onboarding, but the FMP failed to further investigate and assess this repetitive information about other websites used by the customer and the services offered there.

Example 8

Customer I is a natural person whose declared activity is e-commerce related to electronic devices. The customer performed 900 operations over four months, with the value of around EUR 110,000, with over 700 payers and payees. The customer's declared country of birth is Syria and the customer's IP data shows that the customer connects to the account from cities on the Turkish border with Syria (Gaziantep, Mardin, Hatay, etc.), which are associated with a higher risk in terms of both refugees and TF. Although the FMP collected information on the customer's IP addresses, it failed to analyse and evaluate this information in detail, nor did it request that the customer explained the purpose and reasons for his operations.

Example 9

Customer J is a natural person with a declared activity (at the time of onboarding) of a student and later individual activities. Over the first two months of the business relationship, the customer carried out 700 operations with the value of approx. EUR 400,000 with over 550 payers and payees. Around 20% of the customer's payments were made by splitting operations over a few minutes, although the purpose of such splitting is not clear. It should be noted that, although the FMP's monitoring observed the majority of payment operations performed by the customer and determined that the customer's activities were not in line with the ones declared by the customer and the information in possession of the FMP, no further action was taken to clarify the inconsistencies and to establish the basis and purpose of the customer's operations. The nature of the customer's business and the source of his income were also not properly identified.

Example 10

Customer L is classified as posing a high ML/TF risk, its country of registration is Turkey, and its legal status is that of a legal person. The customer transferred EUR 3 million from its account with a Turkish financial institution to the account opened with the FMP. This payment was suspended, but the FMP stated that the operation was between the company's own accounts, thus, the alert generated was closed without finding suspicion. The FMP failed to assess the source of the customer's funds, nor did it determine whether or not the primary source of the funds came from third parties, in particular in view of the fact that the payment was made from the account of a financial institution located in a third country.

Example 11

Customer M's country of registration is the target territory, and its legal status is that of a legal person. The customer's declared activity is marketing services. Over a two-month period, 85 payments were received in the customer's account from accounts opened with financial institutions in Germany and Austria and belonging to 60 different natural persons. The value of individual operations ranged from EUR 500 to 20,000. Almost all operations had the same purpose, i.e. an identical combination of letters and numbers, e.g. "ABCM55669984". The FMP analysed only two operations performed by the customer, for which the FMP asked the customer to provide only a copy of the payer's identity document and a proof of residential address. After the customer provided the documents, the funds were credited to the account. It should be noted that the FMP failed to investigate the purpose for which the funds were transferred to the customer's account, the origin of the funds, the links between the payer and the customer, whether the payers had actually purchased the goods or services from the customer, etc., as such information was not automatically apparent on the basis of the information collected by the FMP on the customer or on the purpose of the operations.

Example 12

Customer N's country of registration is the United Kingdom, and its legal status is that of a legal person. The customer's declared activity is hosting services. Over a period of three months, the funds entering the customer's account were transferred from individual natural persons. The value of individual operations ranged from EUR 100 to 50,000 and the total value of operations amounted to EUR 2 million. Around 250 different natural persons from various European countries – Belgium, Austria, Germany, the Netherlands, France, Spain, Italy, Portugal, France, the United Kingdom, and others – transferred funds to the customer's account. When monitoring the operations, the FMP only analysed the operations and, having suspended the customer's operations, requested that the customer provided a copy of the payer's identity document and a document evidencing the payer's address. After the customer provided the documents, the operations were completed. In these cases, the copies of the payers' identity documents and the documents evidencing the address provided by the customer do not explain the purpose, nature, economic rationale of the operations or source of the funds, and the FMP credited the operations to the customer's account without having taken measures to investigate them. For example, it did not ask for documents substantiating that the payers had actually purchased the services (e.g. contracts) for which they were paying, did not ask for invoices on the basis of which payments were made, etc. In addition, the FMP received 43 requests for cancellation of initiated operations. The funds received by the customer were transferred to Company R associated with virtual assets and investment, but the FMP failed to investigate what goods or services had been purchased by the customer from Company R, nor did it ask for documents substantiating that the goods or services had actually been purchased/provided and that payment was made specifically for the goods or services delivered. It should be noted that such customer activity may be consistent with a typology where, after collecting funds from many different payers (*many-to-one*), the funds are transferred to another account to obscure the origin of the funds.