Recommendation 5/2025 (VI.16.) of the Magyar Nemzeti Bank

on Information required by financial institutions and their intermediaries on the source of funds, on the presentation of documents regarding the source of funds to verify the submitted information, on facilitating the recognition of data, facts and conditions that serve as the basis of reports, and on actions related to the reporting of transactions of high risk

I. Purpose and scope of the recommendation

The purpose of the recommendation is to formulate the expectations of the Magyar Nemzeti Bank (hereinafter: MNB) with regard to the information related to the source of funds requested by the financial institutions and their intermediaries based on the legislation, the documents related to the source funds for the verification of such information, the fostering of the recognition of data, facts and circumstances underlying the notifications as well as the management of the notification of transactions involving high risk, thereby enhancing the predictability of the application of law and facilitating the uniform application of laws and compliance with the international and domestic standards related to the prevention of money laundering and terrorist financing.

The recommendation does not intend to outline good practices expected in connection with the information related to the source of assets. Although the recommendation also accepts information on the source of assets as evidence of the source of funds in specific cases, the two are not generally equivalent. While concerning the source of funds it is always the source of the specific transaction that should be examined, the declaration related to the source of assets is usually connected to the establishment of the business relationship (rather than to a specific transaction) and includes the sources of income and asset components that are likely to serve as funding of transactions to be executed in the future.

By publishing the recommendation, the MNB intends to reduce financial institutions' risks of money laundering and terrorist financing arising in high-amount cash transactions, in line with the National Risk Assessment revised in 2022/2023 and the findings of the European Commission's supranational risk assessment. The wide-ranging use of cash in financial transactions represents a high level of risk, both in relation to general crimes and the crimes of money laundering and terrorist financing.

The MNB aims to support the activities of financial institutions and their intermediaries falling within Act LIII of 2017 on the Prevention and Combating of Money Laundering and Terrorist Financing (hereinafter: AML Act) by providing them with a consolidated set of alerts of unusual transactions, identified to date by the actors of the sector, affecting the scope of service providers' activities.

The recommendation defines clear actions for the service providers regarding the measures to be taken by them, in addition to the notifications concerning transactions involving high risk.

When preparing the recommendation, the following legal acts were taken into consideration:

- Act CXXXIX of 2013. on the National Bank of Hungary (MNB Act),
- Act LII of 2017 on the Implementation of Financial and Asset-related Restrictive Measures Ordered by the European Union and the UN Security Council,

- Act LIII of 2017 on the Prevention and Combating of Money Laundering and Terrorist Financing (AML Act),
- Decree No. 21/2017 (VIII. 3.) of the Minister for National Economy on the mandatory content elements of an internal regulation to be prepared pursuant to Act LII of 2017 on the Implementation of Financial and Proprietary Restrictive Measures ordered by the European Union and the UN Security Council, and
- MNB Decree 30/2024. (VI. 24.) on the detailed rules for the implementation of certain obligations of service providers supervised by the Magyar Nemzeti Bank pursuant to the Act on Preventing and Combating Money Laundering and Terrorist Financing and on the minimum requirements for the development and operation of a screening system of such service providers pursuant to the Act on the Implementation of Financial and Asset-related Restrictive Measures ordered by the European Union and the UN Security Council

The recommendation is addressed to credit institutions, financial service providers, institutions for occupational retirement provision, voluntary mutual insurance funds, service providers engaged in accepting and delivering international postal money orders and trustees (hereinafter collectively: service providers) supervised by the MNB.

This recommendation does not fully refer to the legal provisions when setting out the principles and expectations, but the addressees of this recommendation remain of course still obliged to comply with the relevant legal requirements.

This recommendation does not provide any guidance on data management and data protection issues, does not contain any expectations regarding the processing of personal data and the requirements contained in this recommendation should not be in any way interpreted as an authorisation to process personal data. Data processing in the context of the fulfilment of the supervisory requirements set out in the recommendation should only be carried out in compliance with the data protection legislation in force at any time.

II. Generally expected practices when obtaining information on the source of funds

1. The MNB considers the provision of information on the source of funds (SoF) and the presentation of documents on the source of funds for the purposes of verifying this information (hereinafter referred to as SoF obligation) as integral and uniform measures. Taking into account the applicable legal obligations and based on the risk assessment approach, the MNB expects that the SoF obligation will be fulfilled in the analysis and assessment of risky transactions of clients affected by the data, facts and circumstances that form the basis of the report submitted pursuant to Section 30 of the AML Act., risky transactions of clients affected by correspondent banking and regulatory inquiries, and transactions identified as risky by the screening systems.

2. In order to ensure that the necessary documents are available at the time of the transaction, the MNB expects the service provider to draw the attention of its customers in advance regarding the cash transactions falling within the scope of the SoF obligation, to the documents that will be required for their completion. When examining the SoF of a transaction initiated outside the premises used for the official purposes of the service provider (typically transfers), the MNB considers it good practice if the service provider sends a written notice to the known electronic (e.g. e-mail, internet banking interface) contact details of the SOF obligated customer in order to present the SOF data, and the service provider sets an appropriate deadline for the fulfilment of the obligation specified in the notice.

3. Upon failure to meet the SoF obligation, the MNB regards it as good practice – in line with the expectations of the AML Act – to deny primarily the execution of the transaction initiated by the customer until such time as the necessary information is obtained. Furthermore, if customer due diligence data are

available – because of an already existing business relationship or an attempted transaction – the MNB also deems it necessary to send a notification to the financial intelligence unit. If the client fulfils the SoF obligation after the notification, the MNB considers it good practice for the service provider to supplement the notification sent to the financial intelligence unit with the new information.

4. The MNB expects the service provider to process and store the document proving the source of funds in accordance with the prevailing data protection legislation, only to the extent necessary for the performance of its tasks related to the prevention and combating of money laundering and terrorist financing. The MNB considers it good practice if the documents presented are preserved in accordance with the provisions of point 8 in such a way, that based on their contents, both the business areas performing the internal defence function and the competent authorities can clearly determine whether the person subject to the SOF obligation has fulfilled her data provision obligation in accordance with the expectations. Such confirmation documents may include, for example, a contract or other official document resulting from inheritance, indemnification, civil law relations, a wage certificate from an employment relationship, a certificate of income from foreign service, other income certificates, a certificate of exchange gains, winnings or dividends. The MNB expects, that if necessary, the service provider should ask for further information.

5. The MNB expects the service provider – when obtaining information on the source of funds – not to accept information provided as the source of funds that relates not to the source of funds but rather to the purpose of use (such as “investment”, “purchase of real estate”, “other miscellaneous business uses”) or to the business activity of the customer (such as “running a guest-house”, “wholesale market sales”, “transportation”, “restaurant owner”), given that such information should not be considered as information on the source of funds.

6. In the MNB's opinion, the mere fact that the funds come from savings is not sufficient to prove the source of funds, in view of the fact than it does not establish the lawful origin of the underlying funds.

7. Where the customer mentions savings when obtaining information on the source of funds, the MNB expects the service provider to obtain additional data on the customer’s activity that was instrumental in realising such savings from a lawful source.

8. As regards the proof of the lawful source of the savings, the MNB expects the service provider to process and store the document proving the source of funds in accordance with the prevailing data protection legislation, only to the extent necessary for the performance of its tasks related to the prevention and combating of money laundering and terrorist financing. The MNB considers as a suitable document, among other things, the presentation by the customer and the retainment by the service provider of the following original documents logically fitting in with the information, and made out to the name of the customer, in particular:

- a final court or administrative decision (e.g. a grant of probate) not older than 5 years;
- an official certificate (e.g. a land or real estate administrative department) not older than 5 years;
- other public instrument or private deed of full probative value (e.g. on the sale of real estate or motor vehicle, gift) not older than 5 years,
- a payment account statement (bank account statement) and a cash withdrawal voucher (when the customer cannot provide a statement of the payment account or a bank account statement, because it is not available, the cash withdrawal voucher), not older than 3 years;
- a certificate of winnings not older than 1 year, issued by a gambling company;

• employer's certificate of salary, dividends, bonuses not older than 6 months;

9. If - based on the reasonable rationale presented by the customer and accepted upon careful consideration by the service provider - the documents mentioned in point 8 are not available, the MNB considers acceptable – for the purposes of certification up to the amount of HUF 100 million – a declaration by the customer in a private deed of full probative value on the source of the funds and the reason for the absence of the documents specified above. The MNB regards it as good practice for the service provider to restrict this possibility to those transactions of its customers who have previously made a declaration related to the source of funds that are in line with the content of the declaration.

10. The MNB will deem the SoF obligations to have been fulfilled, if the service provider has official knowledge of this even without a request for information. In application of this recommendation official knowledge should include the cases where the source of funds have been verifiably managed by the service provider before, or where the service provider has authentic documentation on the background thereof, including in particular a statement on the source of the assets, which also includes the asset component that serves as the source of the funds involved in the transaction. The MNB considers it good practice for the service provider to obtain SoF information not for all transactions of a high-risk customer, but only for those transactions for which the service provider does not have knowledge - in line with the level of risk - of the lawful source behind the transaction. In the MNB's view, many transactions may, by their nature, be exempt from the SoF obligation (e.g. wage-type payments, payment of bank fees or public charges, recurring framework-type payments, if the framework contract underlying them is known to the service provider).

11. The MNB expects the service provider to compare in all cases the data obtained with other data available on the customer. If any doubt arises concerning the verity or authenticity of the data, the MNB expects the service provider to report the transaction to the financial intelligence unit without delay and to record the fact of the notification supported by documents. When obtaining SoF information, the service provider is particularly expected to know the economic purpose and nature behind the customer's transactions and to be convinced of their rational nature. It is therefore expected that the service provider will obtain SoF information even if the customer's account turnover is not supported by the economic activity related to the transactions carried out or the services used (i.e. its rational economic nature is not apparent), for example, it is not clear why the customer establishes or maintains a business relationship in Hungary even in the absence of visible economic benefit. In such cases, in addition to the SoF information, the service provider is expected to obtain from the customer the information that is suitable for supporting the lawful nature of the transactions carried out or the services used by the customer.

III. Facilitating the detection of data, facts and circumstances underlying the notifications

12. The MNB expects the service provider to apply and issue alerts to its employees concerned in order to facilitate the detection of data, facts and circumstances underlying the notifications to be submitted to the Financial Intelligence Unit.

13. The MNB considers it good practice to send a report to the service provider's AML/CFT compliance officer[1] at least every two weeks, based on which the riskiest, potentially money laundering or terrorist financing phenomena identified by the service provider can be monitored. The MNB considers it good practice for the service provider to include, among other things, reports submitted to the financial intelligence unit, including data on customers reported repeatedly and the measures taken in relation to

[1] For AML/CFT compliance officer see MNB Recommendation 3/2024. (V.24.) on the officers responsible for ensuring compliance with the fight against money laundering and terrorist financing, their duties and responsibilities, and the related internal procedures and controls.

them, screening alerts, including data on customers included in the most alerts or involved in the largest transactions and the measures taken in relation to them, customer relationship restrictions, the development of the number of customers classified as risky, the development of transfers between the countries most affected by cross-border payment transactions, the development of inquiries from correspondent banking and money laundering and terrorist financing prevention authorities, the presentation of modifications made to the screening system and a general presentation of newly identified risky phenomena.

14. The Annex to the recommendation contains a list of the alerts that the MNB deems important and that warn of unusual transactions affecting the scope of the activity of the service provider falling within the AML Act. The MNB expects the service provider to take into consideration the presented alerts during its internal risk assessment and upon developing its filtering and notification practices based on that. The list is not exhaustive, and in addition to the cases listed therein, the service provider should use additional alerts based on its own risk assessment during the filtering performed by it and upon developing its notification practice.

15. In order to ensure a reinforced procedure for reported customers, as well as for the reinforced procedures applied with regard to reports submitted to the financial intelligence unit, the MNB expects the service provider to establish controls from which the need for repeated reporting can be monitored, and the necessary action can be ensured by the AML/CFT compliance manager.

16. The MNB expect that upon receiving an inquiry from the supervisory authorities the service provider should justify why it failed to send a notification despite the alert included in Annex 1 of this recommendation.

17. The MNB expects the service provider to notify the MNB if it deems justified to amend the list in Annex 1 to this recommendation due to new types of unusual transactions observed by it and that are subject to notification.

IV. Measures related to transactions involving high risks

18. The MNB expects the service provider to:
a) examine in a documented manner the need to terminate the business relationship, or
b) other methods of risk mitigation (e.g. restricting the services to providing only basic account services, termination of contracts for risky products, etc.), if

i four further notifications have been made in relation to the customer within one year from the last notification, or
ii if the amount of transactions included in the notifications relating to the customer exceeds HUF 500 million, or
iii if the financial intelligence unit has informed the service provider that the termination of the business relationship would not jeopardise the conduct of the analytical and evaluation activity.

19. Documentation of the de-risking of the business relationship is also required in cases where the risks contained in the report sent to the service provider's AML/CFT compliance officer as set out in point 13 make it necessary.

20. The MNB expects that based on the examination conducted as a result of the circumstances specified in points 18 and 19 the service provider establishes a committee with the participation of the business and control areas, if the AML/CFT compliance officer deems it necessary to obtain further professional aspects to support its decision whether the business relationship may be maintained.

21. The MNB regards it as good practice to select the members of the committee referred to in point 20 from among the employees managing the various business units of the service provider. It is expected that the AML/CFT compliance officer appointed pursuant to Section 63(5) of the AML Act is a member of the committee, and it is ensured in the internal procedures governing the work of the committee that, if the AML/CFT compliance officer deems it necessary, he may also consult with the responsible manager appointed pursuant to Section 63(4a) of the AML Act before making a decision.

22. The establishment of the committee may be waived if the number of employees of the service provider is below 50. In this case, the MNB regards it as good practice that based on the result of the examination conducted based on the circumstances under point 14, the manager designated in Article 63(5) of the AML Act should decide alone whether the business relationship can be maintained. The MNB expects the service provider to make a decision on maintaining the business relationship in writing within 30 days of (i) sending a notification to the financial intelligence unit or (ii) receiving a notification from the financial intelligence unit. The decision is expected to include – if any – the minority dissent and its reasons, as well as all circumstances that serve to support the decision.

23. The MNB expects the service provider to carry out a repeated examination 1 year after the decision to maintain the business relationship with the given client– if the AML/CFT compliance manager deems it necessary, by convening the committee - to decide on the termination or maintenance of the business relationship, or on another method of risk mitigation, and also on whether the investigation needs to be re-conducted after one year in the absence of a new report.

24. The MNB expects the service provider to retain the documents related to the examination and the decision for eight years in accordance with the data retention rules of the AML Act and the prevailing data protection legislation.

V. Closing provisions

25. The recommendation is a regulatory instrument, issued in accordance with Article 13(2)i) of the MNB Act, with no binding force on the supervised financial organisations. The content of the recommendation issued by the MNB explains the statutory requirements, the principles proposed to be applied based on the MNB's law enforcement practice as well as the methods, market standards and practices.

26. In line with the general European supervisory practice, during its audit and monitoring activity the MNB monitors and assesses compliance with the recommendation by the financial organisations supervised by it.

27. The MNB highlights that credit institutions may make the contents of this recommendation part of their policies. In such case, the financial institution is entitled to indicate that the provisions of its relevant policies comply with the relevant recommendation issued by the MNB. If the credit institution wishes to incorporate only certain parts of the recommendation in its policies, it should not make a reference to the recommendation as a whole or should only do so in respect of the parts taken from the recommendation.

28. The MNB expects the respective financial institutions to apply this recommendation from 1July 2025.

29. Recommendation 14/2020 (XII.17.) of the Magyar Nemzeti Bank on Information required by financial institutions and their intermediaries on the source of funds, on the presentation of documents regarding the source of funds to verify the submitted information, on facilitating the recognition of data,

facts and conditions that serve as the basis of reports, and on actions related to the reporting of transactions of high risk is hereby repealed.

Mihály Varga
Governor of the Magyar Nemzeti Bank

CRITERIA FOR DETECTING UNUSUAL TRANSACTIONS

The purpose of this Annex is to facilitate the implementation of the notification obligation specified in Article 30 of Act LIII of 2017 on the Prevention and Combating of Money Laundering and Terrorist Financing (AML Act).

1. Peculiarities arising upon opening an account, concluding transactions or in the customer relationship

1.1 The appearance (e.g. homeless), communication or the background, age, capabilities that may be inferred from the external characteristics of the owner and/or manager of the company are incompatible with the activities of the company.

1.2 The customer provides a non-existent phone number.

1.3 The customer is concerned about the disclosure of data, in particular those connected to identification, the details of the transaction or other parties to the transaction.

1.4 The customer urges and puts pressure on the clerk during the administration, to avoid the prescribed controls.

1.5 A customer who provides minimal, possibly false, misleading information to complicate the controls, or provides data which cannot be easily verified.

1.6 All the circumstances of the case suggest that false documents have been submitted during the administration.

1.7 There is a striking change in the behaviour and lifestyle of the customer compared to before or there is an unexpected change in his business habits or transactions.

1.8 The customer's high-value purchases are inconsistent with his past shopping habits.

1.9 The customer regularly purchases a large volume of precious metals, precious stones, works of art or other high-value items for a significant amount of money.

1.10 Customers who insist on specific, previously defined employees to avoid risk mitigation measures.

1.11 A payment account for a customer at an address that is far from the location of the branch, if a closer branch would be available and there is no logical reason for choosing the farther branch.

1.12 The customer makes several transactions in one day or in a short period of time, which may as well take place in several branches.

1.13 Missing or incomplete data in payment orders, where it may be assumed that the data deliberately were not provided in full.

1.14 The customer tries to bribe or threaten the administrator.

1.15 The customer is not interested in making a profit, and he is unconcerned regarding the degree of the potential risks, commissions and other transaction costs.

1.16 The customer's risk appetite suddenly increases contrary to his usual behaviour.

1.17 Negative information about the customer or any other person or entity associated with the customer that casts doubt on the source or background of the funds underlying the transaction (including previous criminal or civil sentences).

1.18 A foreign citizen intends to open a payment account for a company without indicating a reasonable economic reason.

1.19 Accounts opened in multiple currencies that are not consistent with the information provided by the client about their activities.

2. Unusual cash transactions

2.1 The deposit or withdrawal of an unusually large amount of cash by a natural person, particularly when it is incompatible with the customer's occupation.

2.2 A sudden and significant increase in cash deposits and cash withdrawals by a natural person, company or other entity.

2.3 Customers who make multiple, relatively small cash deposits, but the total value of these deposits is significant.

2.4 Frequent exchange of different currencies.

2.5 Frequent change of denominations of different banknotes in large batches (small denomination to large denomination, or vice versa.)

2.6 High-amount cash transactions on a previously on a previously dormant account.

2.7 Customers who arrive together and simultaneously carry out large cash or foreign currency transactions at the same bank.

2.8 Regular cash transactions immediately below the identification threshold.

2.9 Immediate cash withdrawal and deposit without actual cash movement, in the form of transactions that involve the accounts of several customers.

2.10 Transactions due to which a branch's demand for large denomination banknotes significantly exceeds the average branch demand. Another circumstance to be assessed in this context is when the delivery of large denomination banknotes to the depository from the respective branch suddenly stops.

2.11 Regular cash deposits in high amounts in the form of “bagged cash deposit”

2.12 Large cash transactions are carried out by the same person at several different companies.

2.13 The customer makes a declaration of dubious content on the source of funds or assets.

2.14 The customer executes transactions below the transaction limits associated with the internal risk assessment to avoid the application of more stringent customer due diligence measures.

2.15 The person withdrawing cash from a payment account is accompanied or waited outside the branch by one or several persons.

2.16 The person withdrawing cash from the payment account does not know the purpose or the background of the transactions carried out on the account. He has no knowledge of the content of the documents submitted regarding the source of the transactions.

2.17 The person who withdraws cash from the payment account asks the branch about the execution of transfers before the transaction is credited to the account.

2.18 A customer or payment account with frequent high-amount cash deposits/withdrawals, where the strap of the banknotes has not been opened and have been stamped by the bank or other banks in previous transactions.

2.19 The customer almost never comes to the branch; instead, the cash is deposited to the customer's payment account by cash couriers.

3. Unusual use of ATM

3.1 Transactions as a result of which the utilisation of a particular ATM is very high compared to the utilisation of other ATMs nearby.

3.2 Frequent ATM transactions abroad, especially if preceded by large cash deposits.

3.3 Frequent ATM cash deposits and withdrawals that approach or reach the daily maximum limits.

3.4 Cash withdrawal from a foreign ATM within a short time following foreign/domestic transfers.

4. Unusual transactions on the payment accounts

4.1 A customer has several payment accounts, which is not justified by his business activity, and there are frequent transfers between payment accounts without any rational cause.

4.2 The movement of funds on a payment account held for an enterprise or other organisation implies no business activity, but significant amounts are credited or debited to the payment account.

4.3 The movements of funds on the account of the company are not consistent with the economic background or expected behaviour of the customer.

4.4 Business activity is conducted on a retail bank account for natural persons.

4.5 The cash movements on the payment account held for natural persons are not in line with the customer's income and past transaction patterns.

4.6 Depositing large amounts of money to the same account by several persons.

4.7 Several persons transfer small amounts to the same account, possibly on a regular basis, and such transfers add up to a significant amount. The credited amounts are transferred to a third account.

4.8 Making large deposits on a security or guarantee account, which is offered as collateral by the payment account holder.

4.9 Making deposits to the account, which are then immediately transferred to other accounts.

4.10 Regular, large VAT refunds are credited to the account held for an enterprise.

4.11 Based on the account turnover, the volume of the company's cash flow is not in line with the amount of tax paid.

4.12 A sudden increase in the number or amount of transactions on the customer's payment accounts.

4.13 A change in the company's business activity and, in connection with this, a change in the transactions through the payment account, which is not in line with the company's previous profile.

4.14 Inactive (dormant) accounts held for a company or natural person become active again without any plausible reason.

4.15 The account turnover data imply a frequent change in the company’s business activity. (Based on the account turnover data, you find that the account holder company used to have relations with e.g. food trading companies; however, suddenly companies engaged in the trading of IT equipment have become its main business partners).

4.16 A high-amount credit transfer is followed by a cash withdrawal on the same day or the next banking day.

4.17 “Chain transfers”:

- at the front of the transfer chain there is a company that pursues real economic activity (website, real registered office, business sites, business partners),
- involving several companies, they make parallel transfers on several payment accounts,
- credits and debits to the payment accounts of the companies in the chain are usually made within a day or within one or two days, in the same or similar amounts,
- the credit entry comes from the same company and the debit entry is made to the same company,
- the funds are transferred abroad or withdrawn in cash from the payment account of the company(ies) being the last resident member of the transfer chain,
- continuous replacement of the last company(ies) in the transfer chain, which may as well happen monthly or quarterly, with the other members of the chain remaining constant.

4.18 There are no transfers in the payment account that would imply normal economic activity (e.g. wage payments, utility bills).

4.19 Significant amounts are paid to the payment account of the company, in cash, on behalf of non-resident companies.

4.20 High-amount credit transfers are received as a result of transactions carried out by Hungarian citizens on behalf non-resident companies from a payment account held with a resident credit institution.

4.21 High-amount credit transfers are received from abroad, from non-resident companies, the members of which and the persons authorised to sign for the company are Hungarian citizens.

4.22 Cash deposits to a payment account held with a resident credit institution for a non-resident company, followed by high-amount transfers to the payment accounts of resident companies.

4.23 High-amount transactions of companies with counterparties with suspended or cancelled tax number, or subject to compulsory strike-off (or previously related to such companies), particularly when the aforementioned risky companies regularly replace each other among the suppliers.

4.24 The payment account was newly opened or had been a dormant account for a long time. The payment account receives (a) significant transfer(s) worth several hundred thousand EUR without any prior history, or after a so-called test transfer of 100-200 EUR, which are immediately transferred to (an) account(s) held in a third country. The account(s) held in a third country could previously be linked to the data, facts and circumstances that served as the basis for the report.

5. Unusual transactions of companies

5.1 The owner and/or senior executive of the company changes and the new owner's/senior executive’s appearance (e.g. homeless), communication or background, age, skills implied based on his external characteristics are incompatible with the company's activities, or the company's financial activities suddenly change following the change of owner/senior executive.

5.2 A company the financial indicators of which significantly differ from those of similar companies without any rational explanation or justification.

5.3 Transactions where the difference between the customer's address (residence), registered office (branch, business site), usual business activity and the place of the transaction (including the place of order, execution, performance, etc.) cannot be explained by the information available about the customer.

5.4 On the same day, several deposits are made to the company's payment account at different bank branches.

5.5 A payment account to which transfers are made that are inconsistent with the account holder company or its previous activities or that do not have a rational business justification (outgoing and incoming transfers, particularly to and from off-shore territories).

5.6 A payment account to which a large number of small credit entries are received or to which cash is deposited in several smaller amounts adding up to a large amount, and the total amount credited to the account is subsequently transferred, provided that this activity is inconsistent with the customer's former activity.

5.7 The company often makes large cash deposits, its payment accounts have a high balance, but it does not use other services.

5.8 Unusual transfers of funds between related payment accounts or on the payment accounts of companies with clear ownership relations in addition to the economic relationship.

5.9 The degree, location and frequency of cash deposits are inconsistent with the company's activities.

5.10 The company's senior executive (person authorised to sign for the company) is a person whose appearance, communication or background and skills, as it can be inferred from his external features, clearly do not make him suitable to manage the company, especially if the person who is authorised to dispose over the payment account is not employed by the company.

5.11 The same person or group controls the payment account(s) of several companies and there are regularly unusual movements of funds in the accounts.

5.12 There are frequent transfers from the account with reference to frustrated contracts or erroneous transfers.

5.13 Following its establishment, a company with minimal capital transacts outstandingly high turnover and receives large amounts of loans from other financial service providers.

5.14 Regular and unjustified equity loans granted to the company, if those are of unusually high amount.

5.15 Intraday overdraft facility, which is transferred in one sum to private companies being in ownership and financing relationship with each other, without real economic substance, and at the end of the day the amount is returned to the payment account of the company that initiated the transfer.

5.16 Large bonus payments that are not consistent with the customer's past financial behaviour.

5.17 Frequent transactions, exhausting the maximum daily limits (e.g. withdrawing money from ATM, transferring money via the netbank).

5.18 Companies whose activities cannot be linked to Hungary and whose payment accounts are engaged in transit-type activities (credits received from an account held abroad are transferred to accounts also held abroad within a short period of time, and the amount of credits and debits within a given period is almost the same) based on which the rational reason for opening an account in Hungary is doubtful. Transactions related to the actual operation of the company (e.g. payroll, utility fees, rental fees) do not take place on the payment account.

5.19 Issuing securities in high value, that is not consistent with the customer's business activity.

6. Unusual investment transactions

6.1 Increased demand for investment services in cases where the lawful source of the amount to be invested cannot be proven or the use of the investment service is inconsistent with the customer's business activity.

6.2 Purchases of large volume of securities for cash or purchases in several tranches below the identification threshold.

6.3 Buying, selling or holding securities without justification or under unusual circumstances, e.g. the sale is not justified by the financial situation of the company.

6.4 The sale or purchase of illiquid securities for which there is no established market price, or the price cannot be verified or it is difficult to verify from a public source, or the price is highly volatile and the transaction or series of transactions do not fit the customer's profile.

6.5 An order for derivatives where the customer persistently realises only profits or only losses usually vis-a-vis the same group of ordering counterparties.

6.6 The initiation of a complex transaction involving many accounts and companies, which does not fit the customer's profile, where the series of transactions also include orders related to securities.

6.7 Regularly placing orders for loss-making transactions, especially if the contact person explicitly draws the customer's attention to this.

6.8 Submitting transaction orders, initiated by a high volume of cash deposits.

6.9 Submission of related transaction orders by several, affiliated, customers (usually companies); execution of cross trades.

6.10 Several securities accounts held by the same customer, which do not show significant individual turnover, but the total invested amount is significant.

6.11 A customer who holds an unreasonably large amount or volume of physical securities, despite the possibility of storing the securities electronically.

6.12 After sales, the proceeds are withdrawn or transferred, followed by the submission of a transaction order for a similar or even larger volume after another cash deposit.

6.13 Costly restructuring of the investment portfolio without a reasonable explanation.

6.14 Buying and selling unlisted securities at large price difference within a short period of time.

7. Unusual loan transactions

7.1 Initiating the conclusion of a credit agreement/loan contract against collateral where the origin of the collateral is unknown or the collateral is not in line with the financial situation of the customer.

7.2. Applying to a financial institution for funding when the source of the customer's financial contribution is unknown.

7.3 Initiating the conclusion of a credit agreement/loan contract while there is a significant amount of available funds on other accounts of the customer.

7.4 Utilisation of funds from a loan in a manner that does not correspond to the stated loan purpose.

7.5 Loan application submitted on behalf of an offshore company, or loan application secured by the bonds of an offshore bank.

7.6 The loan purpose stated by the customer has no economic sense, or the customer proposes to provide cash collateral for the loan while refusing to disclose the purpose of the loan.

7.7 The customer secures the transaction by cash deposit.

7.8 The customer uses cash collateral deposited with an offshore financial institution to obtain the loan.

7.9 The funds from the loan are unexpectedly transferred to an offshore territory.

7.10 The own resources necessary for taking a loan is received from an offshore territory.

7.11 The customer unexpectedly repays the loan or a large part of it, without any prior economic event perceived by the service provider.

7.12 Borrowing under high cash collateral or large prepayments before maturity, where the source of the funds is not obvious or it is not clarified.

7.13 The loan is repaid by a person with whom the customer had (has) no financial relationship.

7.14 The borrower or his agent buys property without previous viewing or knowing its true value or purpose.

7.15 The borrower buys several properties in a short period of time, or sells and buys back the same property for no apparent reason.

8. Unusual transactions related to credit cards

8.1 A transfer is received on the credit card from a region specified in point 3 of Annex 2 to MNE Decree 21/2017 (VIII. 3.) or from a bank in such region.

8.2 The top-up of the credit card performed by a large volume of cash or foreign currency.

8.3 High-amount refunds from merchants related to purchases with no previous debit transactions.

9. Unusual international transactions

9.1 Maintaining a large account balance not consistent with the customer's normal business turnover and then transferring the amount abroad.

9.2 A customer who regularly departs from the payment methods customary in the respective countries in the course of his foreign trade activity.

9.3 Transactions of a company with complex ownership structure or where the identity of the beneficial owner cannot be clearly established.

9.4 A customer with a large volume of financial transactions with countries widely known of being associated with drug production or trafficking, especially if the customer's business profile differs from the economic and commercial structure of those countries.

9.5 Transactions involving “shell” (fictitious) banks, the names of which may be very similar to those of a large legal financial institution.

9.6 Frequent or high-amount transactions involving an offshore bank, and these transactions are not consistent with the known economic activity of the customer.

9.7 The customer sends and receives transfers to and from offshore territories, particularly when there is no business reason for such transfers or if such transfers are not consistent with the customer's economic activity.

9.8 The company carries out transactions which are not transparent due to international interpenetrations and are conducted through Hungary only in financial terms, while the movement of goods cannot be traced and verified.

9.9 Regular recurring transfers from the payment account(s) of a natural person to offshore territories.

9.10 Transfers to or from “OSA”or “NRA” accounts.

10. Peculiarity resulting from lack or inadequacy of cooperation

10.1 A company that is reluctant to provide full information about the company's business purpose, previous banking relationships, senior officers, directors or place of business.

10.2 A customer who does not cooperate in obtaining from him the information and documents required for customer due diligence.

10.3 The customer does not cooperate in providing information about the source of funds or makes a statement of dubious content.

10.4 The potential borrower is reluctant or refuses to specify the purpose of the loan or the source of repayment, or specifies a questionable purpose and/or source.

10.5 A customer who provides minimal or questionable information, or provides information that cannot be easily verified by the bank.

10.6 The prospective customer is reluctant or refuses to provide references, or the references cannot be verified or contacted.

10.7 A person who, despite a call to this effect, fails to indicate past or present employment in the loan application.

11. Unusual transactions related to life insurance

11.1 In the case of either a natural person or a legal entity, a significant increase in extraordinary top-ups or withdrawals within a short period of time.

11.2 Significant cash payments not matching the customer's profile in the case of unit-linked life insurances.

11.3 Regularly concluding transactions immediately below the customer due diligence threshold.

11.4 A company that is reluctant to provide full information about the company's business purpose, previous banking relationships, senior executives or place of business.

11.5 A customer who provides minimal or questionable information, or provides information that cannot be easily verified by the insurer.

11.6 The customer wishes to pay make a deposit and insists on not filling in the required registration or reporting forms.

11.7 In the case a natural person or legal entity, the customer is not concerned about the cost of surrendering insurance contracts before their expiry date.

11.8 Insurance contracts concluded with customers whose permanent residence is in a country other than the country of concluding the transactions, without a reasonable economic relation to that country.

11.9 Unidentified beneficiary, or the beneficiary is resident in a high-risk third country.

11.10 Frequent transfers of amounts to new contracts, other accounts, other beneficiaries without a self-evident reason.

11.11 Shortly after concluding the contract, the beneficiary is changed and the circumstances of the case do not provide a reasonable explanation for the change.

11.12 The customer takes out an insurance contract the payment of which clearly exceeds his financial means or it falls outside his needs.

11.13 When using insurance brokers, a cash payment is made to the insurer.

11.14 Cash payments made in respect of an insurance contract not owned by the payee, with the exception of payments made by a close relative.

12. Peculiarities related to currency exchange activity

12.1 The customer holds an unusually large amount of cash and the amount of cash is not consistent with the customer's appearance and behaviour.

12.2 Regular, high value currency exchange.

12.3 The customer does not cooperate in providing information about the source of funds or makes a statement of dubious content.

12.4 Customers who arrive together and simultaneously carry out currency exchange transactions in high amounts.

12.5 Successive transactions immediately below the identification threshold.

12.6 Exchange of rarely used currencies in high amounts or regularly.

12.7 A customer who is reluctant to submit himself to customer due diligence.

12.8 The customer deliberately executes transactions below the transaction limits associated with the internal risk assessment in order to be subjected to a more relaxed assessment and less stringent customer due diligence measures.

12.9 Exchanging small currency denominations to larger denomination, or selling it, or buying another currency simultaneously.

13. Peculiarities related to the use of safe deposit box services

13.1 One or several customers visit the safe frequently.

13.2 The customer visits the safe after withdrawing a large amount of cash.

13.3 A customer rents several safe deposit boxes simultaneously.

13.4 The safe deposit box service is used by a customer who does not live or work in the respective area.

13.5 Those disposing over the safe deposit box have no obvious business or personal relationship with each other.

14. Peculiarities related to pawnbroking activity

14.1 Customers who suddenly repay their pawn loans.

14.2 Customers who regularly pawn large quantities of articles of smaller value individually, but which represent a high amount together, and typically fail to redeem those.

14.3 Customers whose appearance gives rise to the suspicion that the pawned article is not owned by them.

14.4 The customer's clothing or behaviour is not in line with the quality or value of the pawned article.

14.5 The customer changes his mind when he is informed on the identification requirement.

14.6 The customer buys depository receipts and uses them as collateral for the loan.

14.7 A person other than the one who pawned the article tries to redeem a high-value pawned article without a reasonable explanation.

15. Possible indicators of suspected budgetary fraud

15.1 In connection with the customer

15.1.1 A company maintains several accounts with several resident and non-resident financial service providers for no obvious reason.

15.1.2 The person authorised to sign for or represent the company has insufficient knowledge of the activities of the company represented by him (e.g. no information on potential business partners, expected sales revenue, profits, number of employees)

15.1.3 The person authorised to sign for or represent the company has insufficient knowledge of the products he claims to distribute and of the markets of those products and cannot answer by himself the questions asked when opening the account.

15.1.4 The occurrence of the "missing trader" VAT fraud is primarily related to trade in the following types of goods and activities:

- wholesale trade,
- all valuable, individually not identifiable, non-perishable goods, transportable in large volume,
- wholesale of food, sugar and confectionery,
- trading in energy sources, primarily in natural gas,
- wholesale of electronic and other household goods, computer, software, electronic and communication equipment and parts,
- labour market services (labour leasing),
- advertising, publicity, film production, distribution,
- trade in agricultural products not subject to reverse charge on VAT,
- trade in steel and other metal products.

15.1.5 The turnover on the company's payment account is inconsistent with the nature of its activity.

15.1.6 The managing director of the company, who is a foreign national and a permanent resident, has no registered residential address in Hungary, only the data related to the service agent has been registered; the service agent performs this function for several companies.

15.1.7 The place of residence or abode of the senior executive and/or of the person authorised to dispose over the payment account, and the place of business as well as the place of opening the payment account and executing transactions is in a region other than where the registered office of the company is located.

15.1.8 The registered office of the company is at the address of an undertaking providing registered office services.

15.1.9. The same person opens a payment account on behalf of several legal entities simultaneously or overall. (The development of business networks is usually accompanied by the establishment of several companies simultaneously, which may be accompanied by simultaneous opening of accounts).

15.1.10 The company and/or additional companies that may be linked to the member, senior executive or beneficial owner of the respective company are shown in the database on the NTCA's

website under the “Taxpayers with tax deficit, arrears or under enforcement”, the “Suspended tax numbers” or “Tax numbers cancelled as a sanction” menu items and they execute regular, high-amount transactions in connection with their payment account (business chain VAT frauds are usually accompanied by “missing” traders, unavailable to the tax authorities or taxpayers with tax deficit and may as well be subjected to enforcement procedure, and thus they are quite likely to appear in these databases).

15.2 Transaction-related

15.2.1 Making deposits to the account, which are then immediately transferred to other accounts.

15.2.2 VAT refunds the volume of which is not in line with the level of commercial activity.

15.2.3 Regular cash withdrawals in steadily high amounts.

15.2.4 A sudden increase in the number or total value of transactions.

15.2.5 A change in the commercial activity and in related the transactions, which are not in line with the company's previous profile.

15.2.6 Frequent changes in the business area based on changes in the account turnover data (e.g. based on the turnover data of the payment account, you find that the company used to enter into deals with companies trading in food products, but suddenly it started to have business partners engaged in trading with IT equipment).

15.2.7 The credit transfer is followed by a cash withdrawal on the same day or the next banking day.

15.2.8 The person withdrawing cash is accompanied or waited outside the branch by one or several persons.

15.2.9 The person withdrawing cash does not know the purpose or the background of the transactions orders.

15.2.10 The person who withdraws cash asks the branch about the execution of the transfer before the transaction is credited to the account.

15.2.11 Chain transfers:

- At the front of the transfer chain there is a company that pursues real economic activity (website, real registered office, business sites, business partners),
- Involving several companies, they make parallel transfers on several payment accounts,
- Credits and debits to the payment accounts of the companies in the chain are usually made within a day or within one or two days, in the same or similar amounts,
- The credit entry comes from the same company and the debit entry is made to the same company,
- The funds are transferred abroad or withdrawn in cash from the payment account of the company(ies) being the last domestic member of the transfer chain,
- Continuous replacement of the last company(ies) in the transfer chain, which may as well happen monthly or quarterly, with the other members of the chain remaining constant.

15.2.12 There are no transfers that would imply normal economic activity (e.g. wage payments, utility bills).

15.2.13 To the payment account of a company pursuing genuine economic activity:

- Significant cash amounts are paid on behalf of non-resident companies,
- High-amount credit transfers are received in transactions carried out by Hungarian citizens on behalf of non-resident companies from a payment account held with a resident credit institution,

- The credit transfer is received from abroad, from non-resident companies, the members of which and the persons authorised to sign for the company are Hungarian citizens.

15.2.14 Cash deposits to a payment account held with a resident credit institution for a non-resident company, followed by transfers to the payment accounts of resident companies.

15.2.15 Customers transacting a large volume of payments with counterparties whose tax number has been suspended or cancelled or are subject to compulsory strike-off.

16. Indication of suspicious transactions with crypto asset services

16.1. Risks upon establishing a business relationship

16.1.1 Use of straw men: based on the personal appearance of the client, it is clear that he is acting under the direction of an outsider, for example, during the transaction he appears only when identifying himself, or another person makes a statement on his behalf.

16.1.2 Incomplete information on behalf of a legal entity: the person acting on behalf of the client does not have complete information about the company, or perhaps provides false or misleading information about the company's activities.

16.1.3. Providing false data: the customer provides false data or incorrect information about himself or his activities.

16.1.4. Refusal to identify: the customer does not wish to undergo an identification process or withdraws from entering into a business relationship when informed about the mandatory customer due diligence procedures.

16.1.5. Lack of data required for customer due diligence: the customer does not cooperate, so it is not possible to obtain the mandatory data.

16.1.6. Concealing the identity of the beneficial owner: the customer's representative falsely states the identity of the beneficial owner and is unable to substantiate the information contained in the declaration.

16.1.7. Refusal to answer questions regarding the source of wealth: the client does not wish to disclose the origin of funds, virtual currencies or provides manifestly false information.

16.1.8. Citizen of a third country with strategic deficiencies: the client or its beneficial owner is from a third country with strategic deficiencies.

16.1.9. Subsidiary from a third country: the client is a subsidiary of a company registered in a third country with strategic deficiencies.

16.1.10. Large initial deposit: the client makes a significant initial deposit that does not fit his profile.

16.2. Risks arising during the existence of a business relationship

16.2.1. Third party assignment: the beneficiary of the received funds during the sale of a virtual currency is not the customer, but an outside party.

16.2.2. Unjustified cash payment request: the customer wishes to pay the purchase price in cash without providing a reason.

16.2.3. Refusal to verify the source of cash: the customer does not provide a statement on the source of the cash or is unable to provide appropriate documentation.

16.2.4. Entry of a member with a non-transparent ownership background: a new member appears in the customer's organization whose ownership background cannot be verified.

16.2.5. Representation of officers residing abroad: the senior officers of the client organization reside abroad, and another person acts in their place at the Service Provider.

16.2.6. Unavailability of the manager: the client's manager is not available to the service provider.

16.2.7. Lack of logical economic purpose: the economic purpose of the transaction is unsubstantiated or illogical.

16.2.8. Use of mixer or tumbler services: the virtual currency transaction involved the use of a mixer or tumbler service, which helps to conceal illegal sources.

16.2.9. Transactions linked to darknet and illegal activities: the client's transaction may be linked to darknet marketplaces or other illegal activities.

16.2.10. Domain name registration via proxies: users register their domain names via proxies to hide their owners.

16.2.11. Multiple wallets from the same IP: a large number of seemingly independent virtual wallets are controlled from the same IP or MAC address.

16.2.12. Use of virtual currency exchange machines despite high fees: the customer uses virtual currency exchange machines or kiosks with the help of intermediaries (money mules) or scam victims.

16.2.13. Addresses linked to fraud or banned addresses: the customer makes a payment transaction with addresses linked to known fraud, extortion or ransomware.

16.2.14. Funds originating through intermediaries (mixers): the client's funds arrive through a mixer service, which may indicate the concealment of an illegal source.

16.2.15. Use of shell companies: The emergence of shell companies whose purpose is to conceal the actual financial movements.

16.2.16. Lack of transparency in ICOs: the client holds funds originating from ICOs where the data of the investors is not accessible.

16.2.17. Disproportionate wealth from virtual currencies: a significant part of the client's wealth comes from virtual currencies originating from service providers that do not apply measures against money laundering and terrorist financing.

16.2.18. Multiple high-value transactions within a short period of time: a series of high-value transactions that are repeated in a layered manner over time.

16.2.19. Complex transactions to high-risk countries: the customer is conducting a complex transaction to a person or entity whose residence is in a country that raises proliferation concerns.

16.3. Risks arising from the termination of a business relationship

16.3.1. Request for assistance in a breach of law: the client places an order that would constitute a breach of law.

16.3.2. Relationship terminated due to lack of customer due diligence data: the business relationship was terminated because the client did not cooperate during the due diligence process.