MNB recommendation No 15/2022 (IX. 15.)

on the assessment of money laundering and terrorist financing risks and the definition of related measures

I. Purpose and scope of the recommendation

The purpose of this recommendation is to outline the expectations of the Magyar Nemzeti Bank (hereinafter: MNB), and thereby to increase the predictability of the application of the law and to facilitate the uniform application of the relevant legislation in relation to the identification of the factors to be taken into consideration by credit institutions, financial service providers, institutions for occupational retirement provision, voluntary mutual insurance funds, entities accepting and delivering international postal money orders and fiduciaries supervised by the MNB during the assessment of money laundering and terrorist financing (hereinafter: ML/TF) risks attached to the establishment of business relationships or to the execution of transactions. The recommendation also defines how the respective financial institutions should determine the level of their customer due diligence measures to ensure that they are proportionate to the ML/TF risk identified by them.

By publishing this recommendation, the MNB aims to provide tools that helps the respective financial institutions develop their internal risk assessment in line with the requirements of the risk-based approach in the course of their activities performed to prevent money laundering and terrorist financing (hereinafter: AML/CFT) also in a specialised manner at the level of individual clients.

When elaborating the recommendation, the MNB took into consideration the revised Guidelines on Money Laundering and Terrorist Financing Risk Factors published by the European Banking Authority (hereinafter: EBA) on 1 March 2021[1] (hereinafter: Guidelines), which supersede and replace Guidelines JC/2017/37 published by the European Supervisory Authorities (hereinafter: ESA)[2] (hereinafter: ESA Guidelines).

The applicable EU regulatory environment, effective at the time of the publication of the ESA Guidelines, has changed[3]and new AML/CFT risks have been identified, which together justified the revision and repeal of the ESA Guidelines. The Guidelines aim to provide an accurate and up-to-date presentation of the expectations and best practices for the new types of AML/CFT risks, also bearing in mind the changed regulatory environment. Setting out from the requirements outlined in the Guidelines, the MNB defines in this recommendation the practice to be followed by the respective financial institutions.

The recommendation focuses on the identification and assessment of the risks of certain business relationships and transaction orders, which the relevant financial institutions should take into consideration during the risk assessment they are expected to perform based on Article 27 of Act LIII of 2017 on the Prevention and Combating of Money Laundering and Articles 25–31 of MNB Decree No 26/2020 (VIII. 25.) on the detailed rules concerning the implementation of the Act on the Prevention and Combating of Money Laundering and Terrorist Financing, as applicable to service

---

1 https://www.eba.europa.eu/sites/default/documents/files/document_library/Publications/Guidelines/2021/Guidelines%20on%20ML-TF%20risk%20factors%20%28revised%29%202021%2002/Translations/1016931/Guidelines%20ML%20TF%20Risk%20Factors_HU.pdf §

2 https://www.eba.europa.eu/sites/default/documents/files/documents/10180/1890686/66ec16d9-0c02-428b-a294-ad1e3d659e70/Final%20Guidelines%20on%20Risk%20Factors%20%28JC%202017%2037%29.pdf?retry=1 §

3 Directive 2018/843/EU, which amended Directive 2015/849/EU, entered into force on 9 July 2018.

providers supervised by the MNB, and concerning the minimum requirements for the development and operation of the screening system under the Act on the Implementation of Restrictive Measures Imposed by the European Union and the UN Security Council Relating to Liquid Assets and Other Financial Interests.

The recommendation is addressed to the credit institutions specified in point 16 of Article 3 of the AML Act and to the financial service providers, institutions for occupational retirement provision, voluntary mutual insurance funds, service providers engaged in accepting and delivering international postal money orders and fiduciaries (hereinafter collectively: service providers) specified in point 28 of Article 3 of the AML Act. The MNB expects institutions for occupational retirement provision, voluntary mutual insurance funds, entities accepting and delivering international postal money orders and fiduciaries to apply only the provisions of Chapter III.

The factors and measures described in this recommendation are not exhaustive, and the respective financial institutions are encouraged to consider other factors and measures where appropriate.

This recommendation does not fully refer back 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 with regard to 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. Definitions

1. For the purposes of this recommendation:

a) countries of higher ML/TF risk: countries which, based on the assessment of the risk factors specified below, represent higher ML/TF risk. This term includes, but is not limited to, “high-risk third countries with strategic deficiencies” as defined in Article 3(31) of the AML Act, the national AML/CFT systems of which are characterised by strategic deficiencies that pose a significant threat to the financial system of the European Union;

b) combined account: a bank account opened by a client, such as a lawyer or notary, to hold funds belonging to his customers. In such accounts, the funds of the principals are mixed, but the principals cannot instruct the bank directly to carry out transactions;

c) inherent risk: the level of risk before risk mitigation;

d) residual risk: the level of risk after risk mitigation;

e) risk: the impact and likelihood of the occurrence of an ML/TF risk;

f) risk appetite: the level of risk that the service provider is ready to take;

e) risk factors: variables that, alone or in combination with each other, may increase or decrease the ML/TF risk of a business relationship or transaction order;

d) risk-based approach: an approach whereby the supervisory authority and the service provider identify, assess and interpret the ML/TF risks to which the service provider is exposed and enforce AML/CFT measures commensurate with such risks;

i) remote contacts or transactions: any transaction or business relationship where the client is not physically present, i.e. not located physically at the same place where the service provider or a person acting on behalf of the provider is situated. This term covers situations where the identity of the client is verified by means of an audited electronic communication device defined in Article 2(1) of the MNB Regulation.

Unless provided otherwise, the additional terms used in the recommendation shall be interpreted in accordance with the provisions of the AML Act and the MNB Regulation.

III. General principles of risk assessment and risk management

III.1 General expectations related to the assessment of ML/TF risks

2. The MNB expects that the risk assessment should consist of two distinct but interrelated steps:
a) identification and assessment of ML/TF risk factors; and
b) specification of the measures associated with the ML/TF risk proportionate to its degree.

3. The MNB expects the service provider to use the risk factors identified by it for the assessment of the general level of ML/TF risk.

4. When assessing ML/TF risks, the service provider may decide to weight each risk factor differently depending on its relative importance.

5. The MNB expects the service provider to develop a comprehensive view of the ML/TF risk factors it has identified, which together determine the level of the ML/TF risk associated with the business relationship and the transaction order.

6. The service provider should use a comprehensive and consistent approach to the risk associated with the situation and take into consideration that, unless otherwise provided by law, isolated risk factors do not necessarily allocate the business relationship to a higher or lower risk category.

7. When weighting the risk factors, the service provider should make an informed assessment of the relevance of the different risk factors associated with the business relationship and the transaction order. For example, the service provider may assign different risk scores to different factors because the client's personal relationship with a country of higher ML/TF risk is less relevant in view of the characteristics of the product requested by him.

8. The service provider should also take into consideration that the weighting of each risk factor may vary by product, client, client category or service provider. The MNB regards it as good practice for the service provider to ensure the following when weighting risk factors:
a) the weighting should not be unduly influenced by a single factor;
b) economic or profit-oriented considerations should not influence the risk rating;
c) the weighting should not lead to a situation where no business relationship can be classified as high risk;
d) the risk classification of clients should be recorded in the IT systems as well and, depending on the risk assessment and the size of the service provider, its updating should be supported by automated IT solutions integrated in the system;
e) the weighting applied by the service provider should never override the statutory provisions, always applicable to situations of high ML risk; and
f) the risk assessment performed by the service provider should not be based solely on automatisms, and the service provider should be able to overwrite automatically generated risk figures as necessary. The reasons for the decision to overwrite the respective scores shall be always recorded in a retrievable form.

9. If the service provider uses automated IT systems to assess risks for the purpose of categorising business relationships or transaction orders, and purchases these systems from an external service provider rather than developing them in-house, it should familiarise itself with the operation of the systems and with the way of combining the risk factors for the calculation of the overall risk score. The MNB expects the service provider to ascertain that the assigned scores reflect its own understanding of the ML/TF risk and that it can demonstrate this to the MNB.

10. The MNB expects the service provider to decide on the most appropriate way of categorising risks. This depends on the nature and extent of the service provider's business activity and the types of ML/TF risks it is exposed to.

11. After having performed the risk assessment and taken into consideration both the inherent risks and the mitigating tools defined by it, the service provider is expected to categorise its business lines and the business relationships and transaction orders of those in its internal risk assessment based on

the perceived level of ML/TF risk.

12. The MNB expects the service provider to collect sufficient information about the prospective client as part of the customer due diligence to ensure that all relevant risk factors have been identified at the start of the business relationship, during the business relationship and before the execution of the transaction order. The service provider is expected to apply additional customer due diligence measures, where necessary, and to evaluate the risk factors identified in this way in order to obtain a comprehensive picture of the risk associated with the respective business relationship or transaction order.

13. For the purposes of point 11, the service provider is not expected to prepare a full client risk profile in relation to transaction orders.

14. The MNB expects the service provider to use the information obtained during the existence of the business relationship for the purpose of risk assessment (dynamic customer due diligence).

III.2 ML/TF risk factors

15. When identifying ML/TF risks associated with business relationships or transaction orders, the service provider shall assess the relevant risk factors, including the identity of the client, the countries or geographical areas in which it operates, the products, services and transactions requested by the client and the channels used by the service provider to provide these products, services and transactions, taking into consideration, among other things, the list of risk factors specified in the AML Act and in Annexes 1 and 2 to the Decree No 21/2017 (VIII. 3.) of the Minister for National Economy regarding the mandatory substantive elements of the internal regulation to be prepared pursuant to Act LII of 2017 on the Implementation of Financial and Asset-related Restrictive Measures Ordered by the European Union and the UN Security Council.

Customer risk factors

16. When identifying the risk associated with its clients – including, among others, the beneficial owners of the clients – the service provider should take into consideration the following risk factors:

a) the business or professional activities of the client and of the client's beneficial owner;

b) the reputation of the client and the client's beneficial owner; and

c) the nature and behaviour of the client and the client's beneficial owner, including whether this may imply an increased risk of terrorist financing.

17. When considering the risk associated with the business or professional activities of the client or of the client's beneficial owner, the following risk factors, among others, may be relevant:

a) The client or beneficial owner has relations with sectors that are generally associated with a higher risk of corruption, such as construction, pharmaceutical industry and healthcare, defence industry, mining and public procurement.

b) The client or beneficial owner has relations with sectors that are associated with higher ML/TF risk, such as certain payment service providers, casinos or precious metal traders.

c) The client or beneficial owner has relations with industries that use large amounts of cash.

d) In the case of a legal entity or unincorporated entity, trust or other type of legal arrangement of a partnership nature (e.g. fiduciary trust, trusts registered abroad), the purpose for which the client has been established and the type of business pursued by it.

e) The client has domestic or foreign political connections, in particular he is a politically exposed person or the beneficial owner is a politically exposed person. The client or beneficial owner has another relevant relationship with a politically exposed person, for example, any of the client's senior executives is politically exposed person, who exercises significant influence over the client or beneficial owner. If the client or the beneficial owner is a politically exposed person, the service provider shall always apply enhanced customer due diligence measures in accordance with Article 16(1)*d)* of the AML Act.

f) The client or his beneficial owner is fills another key position or performs a key public function that may allow him to misuse that position for personal gain. For example, a person in a senior executive who can influence the award of public contracts, a decision-maker member of a highly ranked sports board or sports federation, or a person who can influence the government and other senior decision-makers.

g) The client is a legal entity whose beneficial owner is subject to enforceable disclosure requirements that ensure public availability of reliable information, such as a listed public company that requires disclosure as a condition of listing.

h) The client is a credit institution or financial service provider from a country with an efficient AML/CFT system, acting on its own behalf, and is subject to local AML/CFT supervision, or the client may have been subject to supervisory sanctions or enforcement in recent years for non-compliance with AML/CFT obligations or other statutory requirements.

i) The client is a local government (or equivalent body) or state-owned company from a country of low level of corruption.

j) Whether the background of the client or the beneficial owner of the client is consistent with what the service provider knows about the past, present or planned business activities, turnover of the client's or its beneficial owner's businesses and source of funds.

18. Risk factors relevant for determining the risk associated with the reputation of the client or its beneficial owner:

a) There are adverse media news or other relevant sources of information about the client, for example, allegations of criminal or terrorist activity concerning the client or his beneficial owner. The service provider should determine the credibility of the allegations based on – among other considerations – the quality and independence of the data source and the persistence of such allegations. The service provider should bear in mind that the absence of criminal convictions is not necessarily sufficient to rule out the alleged risks.

b) The assets of the client, the beneficial owner or any person widely known to be associated with them – e.g. based on press reports – have been frozen as a result of administrative or criminal proceedings or accusations of terrorism or terrorist financing.

c) The service provider is aware of the fact that the client or his beneficial owner has been named in reports on unusual transactions in the past.

d) The service provider has in-house information about the integrity of the client or beneficial owner, obtained e.g. through a long-standing business relationship.

19. Upon assessing the risk associated with the nature or behaviour of the client or beneficial owner, the following risk factors may be relevant; the service provider should take into consideration that not all of these risk factors may be obvious from the outset; they may arise only after the business relationship has been established:

a) The client has reasonable arguments for not being able to provide reliable proof of his identity, e.g. because he is an asylum seeker.

b) The service provider has doubts about the authenticity or accuracy of the identity of the client or his beneficial owner.

c) There are signs that the client may try to avoid entering into a business relationship, e.g. the client executes a single transaction or several one-off transactions, while it would be more rational in economic terms to enter into a business relationship.

d) If the client's ownership and control structure is complex or non-transparent, and it is necessary to examine the commercial or legal justification for it.

e) The client issues bearer shares or acts through nominee shareholders.

f) The client is a legal entity or an unincorporated entity acting as a trustee.

g) Changes in the ownership and control structure of the client without a good reason.

h) The client executes complex transactions of unusually or unexpectedly high amount or type, without any obvious economic or apparently legitimate purpose or commercial justification. It may be assumed, for example, that the client is trying to circumvent the threshold specified in Article 6 of

the AML Act. 6. The client asks for unnecessary or unreasonable confidentiality. For example, the client is reluctant to share customer due diligence information or appears to want to conceal the true nature of its business.

i) The source of the client's or his beneficial owner's funds cannot be easily explained by, e.g. his occupation, inheritance or investments. The service provider is expected to review whether the client uses the products or services he applied for upon establishing the business relationship.

j) The needs of the non-resident client could be satisfied better elsewhere. The MNB expects the service provider to clarify the reasons why the client applies for a product or service in the respective country, in particular when the use of the product or service would be more justified in another country. Reliable economic information and legitimate explanation should be obtained as to why the client applies for the respective type of financial service. The service provider should take into consideration that Article 282/A (2) of Act CCXXXVII of 2013 on Credit Institutions and Financial Undertakings (hereinafter: Credit Institutions Act) provides the right for consumers resident in an EEA State to open a basic payment account, but this right only applies if credit institutions are able to comply with their AML/CFT obligations.

k) The credit and debit entries to client's account are only from and to accounts held abroad, domestic transactions are for small amounts and typically for the purpose of paying the expenses connected to the establishment and operation of the company (e.g. lawyer, accounting services, registered office services); the client does not carry out any actual economic activity in Hungary. The economic rationale for opening the account in Hungary should be also examined.

20. The MNB expects the service provider upon identifying the risk connected to the nature and behaviour of the client or its beneficial owner to pay special attention to risk factors that, although not characteristic of terrorist financing, may imply an increased risk of terrorist financing, especially in situations where other terrorist financing risk factors are also present. For this purpose, the service provider should take into consideration at least the following risk factors:

a) The client or his beneficial owner is a person who is included in the list of persons, groups and entities involved in terrorist acts and subject to restrictive measures, or is known to have close personal or professional relations with such listed persons (e.g. because they are related to each other or because he lives in the same household with such a person).

b) Whether the client or his beneficial owner is a person known to be under investigation for terrorist activity, or who has been convicted of terrorist activity, or who is known to have close personal or professional relations with such a person (e.g. because they are related to each other or he lives in the same household with such person).

c) Whether the client carries out transactions involving incoming transfers of funds from or outgoing transfers of funds to countries where terrorist groups are known to operate in their territory and are known to be a source of terrorist financing or are subject to international sanctions. If yes, it is also necessary to examine whether these transfers can be easily explained, e.g. by family or commercial links.

d) Whether the client is a non-profit organisation

e) the activities or management of which are known to favour extremism or terrorism; or

f) the transactions of which are characterised by large transfers of funds to countries of higher ML/TF risk or to high-risk third countries with strategic deficiencies.

g) Whether the client carries out transactions characterised by large movement of funds in a short period of time involving non-profit entities with unclear relations (e.g. having the same registered office, the same representatives or employees, or having multiple accounts under the same name).

h) Whether the client transfers or intends to transfer funds to the persons mentioned in points *a)*and *b)*.

21. The service provider should pay special to the Terrorist Financing Typology of the Financial Action Task Force (FATF), which is regularly updated.

Risk factors related to countries and geographical areas

22. When identifying the risk associated with countries and geographical areas, the service provider should give due consideration to the following factors:

a) the countries of residence or domicile of the client and the beneficial owner's country of residence;

b) the countries in which the client and its owner have their principal place of business; and

c) the countries with which the client and his beneficial owner have business relations, or linked to through financial or legal interests.

23. The MNB regards it as good practice for service providers to take into consideration that the relative importance of the risk factors in each country and geographical area is often determined by the purpose and nature of the business relationship:

a) If the funds used in the business relationship originated abroad, the frequency of crimes connected to money laundering in that country and the effectiveness of the country's legal system are particularly relevant.

b) If the funds come from or are sent to a country in which groups known to be involved in terrorist crimes are operating, the service provider shall consider the extent to which this is likely to give rise to suspicion, based on its knowledge of the purpose and nature of the business relationship.

c) Where the client is a credit institution or a financial service provider, the service provider should pay special attention to the adequacy of the AML/CFT system in the country and the effectiveness of AML/CFT supervision.

d) If the client is established through some other legal arrangement or it is a trustee, or has a structure or function similar to a trustee[4], the service provider should take into consideration the actual extent to which the country of the client's – or where applicable of the beneficial owner's – registered office actually complies with international standards on transparent taxation and information sharing.

24. The MNB is of the opinion that for the purposes of determining the effectiveness of a country's AML/CFT regime, the primary risk factors that a service provider needs to consider include:

a) Whether there is a statutory prohibition on the implementation of group-wide policies and procedures and, in particular, whether there are situations when the service provider applies Commission Delegated Regulation 2019/758/EU[5].

b) It classified the country's AML/CFT system as one with strategic deficiency in accordance with point 31 of Article 3 of the AML Act.

25. Information on the quality of a country's AML/CFT controls –including the quality and effectiveness of enforcement measures and supervision – should be obtained from more than one credible and reliable source of information. Possible sources include, among other things: the mutual evaluation reports of the FATF and its subordinate FATF-style Regional Bodies (FSRBs) (good starting points include: the Executive Summary and key findings, as well as the assessment of compliance with recommendations 10, 26 and 27 and immediate outcomes 3 and 4), as well as the FATF list of high-risk and non-cooperative countries, the assessments prepared by the International Monetary Fund (IMF) and the reports prepared under Financial Sector Assessment Programme (FSAP). The service provider should bear in mind that membership in FATF or FSRB membership alone (e.g. Moneyval membership) does not necessarily mean that the country's AML/CFT system is adequate and efficient. The MNB expects the service providers – to the extent permitted by law – to identify countries of lower risk in accordance with this recommendation and the provisions of Chapter III of the MNB Decree. When identifying the level of terrorist financing risk associated with a country, the service provider should consider primarily the following risk factors:

a) Police intelligence or information from other credible and reliable public media sources indicating that a country provides funding and support for terrorist activities, either from official

[4] Similar structures include fiducies, fideicomiso and Treuhand.

[5] Commission Delegated Regulation 2019/758/EU of 31 January 2019 Supplementing Directive 2015/849/EU of the European Parliament and of the Council with regard to regulatory technical standards for the minimum action and the type of additional measures credit and financial institutions must take to mitigate money laundering and terrorist financing risk in certain third countries.

sources or from organised groups or organisations within the country.

b) Police intelligence or information from other credible and reliable public media sources implying that terrorist groups are operating in the country or territory.

c) Whether the country is subject to financial sanctions, embargoes or other measures imposed by the United Nations or the European Union in relation to terrorism, terrorist financing or proliferation of weapons of mass destruction.

26. When determining a country's level of transparency and tax compliance, the service provider should consider the following risk factors:

a) Information should be obtained from more than one credible and reliable source to demonstrate that the country's tax transparency and reporting complies with international rules and that the relevant rules are effectively implemented in practice. Examples of possible sources include: reports from the Organisation for Economic Co-operation and Development (OECD) Global Forum on Transparency and Exchange of Information for Tax Purposes, which rates countries for tax transparency and exchange of information; assessments of a country's commitment to automatic exchange of information based on common reporting standards; assessment performed by FATF or FSRBs of compliance with FATF recommendations 9, 24 and 25 and immediate outcomes 2 and 5; assessments performed in respect of the EU list of non-cooperative countries from a tax perspective and IMF assessments (e.g. assessment of offshore financial centres performed by IMF staff).

b) Whether the country has committed to and effectively implemented the common reporting standard for automatic exchange of information adopted by the G20 in 2014.

c) Whether the country has reliable and accessible registers on beneficial owners.

27. When exploring the risk associated with the level of predicate crime related to money laundering by country and geographic area, the service provider should consider, among others, the following risk factors:

a) Information from credible and reliable public sources on the level of money laundering-related predicate crimes defined in Act C of 2012 on the Criminal Code – such as corruption offences, organised crime, budget fraud of a more serious category – including corruption perception indices, OECD country reports on the implementation of the OECD Anti-Bribery Convention, and the report of the UN Office on Drugs and Crime on the global drug situation.

b) Information from more than one credible and reliable source on the ability of the country's law enforcement and judicial system to investigate and prosecute these offences efficiently.

Risk factors connected to products, services and transactions

28 When exploring the risks associated with its products, services or transactions, the service provider should consider the risks associated with:

a) the level of transparency or lack of transparency of the product, service or transaction;

b) the complexity of the product, service or transaction; and

c) the value or volume of the product, service or transaction.

29 When exploring the risks associated with the transparency of its products, services or transactions, the service provider should consider the risk associated with:

a) It should be examined to what extent the products or services facilitate the maintenance of the anonymity of the client, the beneficial owner or the beneficial owner structures or support the concealment of their identity. Examples of such products and services include bearer shares, fiduciary deposits, offshore companies and certain trust arrangements that may be structured to take advantage of anonymity and facilitate transactions with shell companies or companies with shareholders holding bearer shares.

b) A third party not involved in the business relationship may give instructions, for example in the case of certain correspondent banking relationships.

30. In relation to the risk associated with the complexity of the product, service or transaction, the following risk factors should be considered:

a) Whether the transaction is complex and involves several parties or several countries. Whether the products or services permit third party payments or accept overpayments even if they usually would not be expected. Upon assessing the risk, it is a risk mitigating factor when the products and services are funded by a transfer from the client's own account held by another credit institution or financial service provider which is subject to AML CFT standards and supervision similar to those prescribed by the AML Act.

b) Whether the risks associated with the new or innovative product or service are known, especially when it involves the use of new technologies or payment methods.

31. In relation to the risk associated with the value or the volume of the product, service or transaction, at least the following risk factors should be considered:

a) Whether the products and services are cash intensive, such as many payment services and certain current accounts.

b) Whether the products and services facilitate or foster transactions for large amounts. Consideration should also be given to maximising transaction value or fee income, as this may restrict the use of the product or service for ML/TF purposes.

Risk factors connected to service channels

32. When identifying the risk related to the manner the client uses the requested products or services, service providers should consider the risks related to:

a) the extent to which the business relationship is managed impersonally; and

b) the intermediaries used by the service provider and their relationship with the service provider.

33. When identifying the risks attached to the manner in which the client uses the product, the MNB expects the service provider to consider, among others, the following factors:

a) Whether the client is physically present at the time of identification. If not, it should be assessed whether the service provider used a reliable form of remote customer due diligence and took measures to prevent misuse of identity. For this purpose the service provider should apply the provisions of points 49–54 hereof.

b) Where the customer due diligence has been performed by another member of the same financial group, it should be assessed to what extent the service provider may rely on that due diligence as an assurance that the client will not expose it to excessive ML/TF risk. The service provider should ascertain that the group member has applied the customer due diligence measures as defined in Article 22(5) and (6) of the AML Act.

c) If the customer due diligence has been performed by a third party not belonging to the same financial group, it should be documented how the service provider has ascertained that:

i. the third party applies customer due diligence measures and maintains records in accordance with EEA requirements and it is supervised in terms of compliance with the AML/CFT obligations in accordance with Article 22(3)*a)* of the AML Act;

ii. whether there are any signs implying that the third party does not comply with the applicable AML/CFT legislation (e.g. whether the third party has been sanctioned for breaching its obligations related to the prevention of money laundering and terrorist financing);

iii. whether the third party is established in a country of higher ML/TF risk. If the third party is established in a high-risk third country with strategic deficiencies, the service provider shall not accept the result of the customer due diligence carried out by the third party, with the proviso that according to Article 22(5) of the AML Act, if a service provider established in Hungary or in another Member State of the European Union wishes to accept the results of customer due diligence from its branch or subsidiary in a high-risk third country with strategic deficiencies, relying on that third party is permitted, provided that such branch or subsidiary complies with the ML/CFT policies and procedures defined at group level pursuant to Article 62 of the AML Act;

iv. upon a written request, the third party presents, without delay, a copy of the identification and due diligence documents, in accordance with Article 23(1) and (2) of the AML Act;

v. the third party's customer due diligence measures are of a quality that can be relied upon;

vi. the level of customer due diligence applied by the third party is proportionate to the ML/TF risk associated with the business relationship, considering that the third party applies customer due diligence measures for its own purposes and possibly in other context;

(vii) the customer due diligence was performed through a tied agent, i.e. not directly at the service provider, it shall be ascertained that the agent has obtained sufficient information to enable the service provider to understand its client and the level of risk associated with the business relationship;

viii. upon using independent or tied agents it should be verified to what extent the agents are involved in the establishment of the business relationship and how this affects the service provider's knowledge obtained about the client and the continuous risk management; and

ix. when the service provider uses, to the extent permitted by law, a service provider rendering outsourcing services to fulfil its AML/CFT obligations, whether it has examined that the outsourced service provider is an obliged service provider under the AML Act or an equivalent regulatory regime and whether it managed the risks specified in Recommendation No 12/2022 (VIII. 11.) of the Magyar Nemzeti Bank on the development and operation of internal lines of defence, management and control functions of financial institutions, if applicable.

III.3 Customer due diligence measures

34. The MNB expects the service provider's AML/CFT policies and procedures to be based on and reflect its risk assessment.

35. The risk assessment performed by the service provider should help it determine where to focus its resources to manage ML/TF risk, when admitting the client and throughout the duration of the business relationship.

36. The MNB expects the service provider's customer due diligence measures to facilitate the identification and assessment of risks associated with business relationships and transaction orders.

37. The MNB expects service providers to specify in their policies and procedures:

a) the identity of the client and, where applicable, the beneficial owner for each client type and for each product and service category, and whose identity is to be verified for customer due diligence purposes. The service provider should take into consideration the sector-specific requirements specified in Chapter IV of this recommendation, which provide further details on the identification of clients and their beneficial owners;

b) what constitutes a transactional order in connection with their business activity and, as part of this, when it actually qualifies as a series of related transaction orders under point 37 of Article 3 of the AML Act. The service provider should take into consideration that the thresholds specified in Article 6(1)*b)* and *d)* of the AML Act are only relevant to the extent that they require the unconditional application of customer due diligence measures; transaction orders even below this threshold may be considered as series of effectively related transaction orders;

c) the level and type of customer due diligence that will be applied to the business relationships and transaction orders;

d) how the identity of the client and, where applicable, the beneficial owner, is to be verified and how the purpose and nature of the business relationship is to be determined;

e) the level of monitoring to be applied under different circumstances;

f) defining the use of the enhanced procedure and its scope, including how and in which situations the use of the enhanced procedure is appropriate to mitigate risks; and

g) the risk appetite of the service provider.

Financial inclusion and de-risking

38. “De-risking” refers to the decision of the service provider not to provide services any longer to certain categories of clients representing higher ML/TF risk. As the risk associated with business

relationships may vary even within a category, the application of the risk-sensitivity approach does not make it necessary for the service provider to refuse to establish a business relationship or to terminate a business relationship with entire categories of clients of higher ML/TF risk. The MNB expects the service provider to find the proper balance between the need for financial inclusion and the need to mitigate ML/TF risk through de-risking.

39. As part of this, the service provider is expected to apply appropriate and risk-sensitive policies and procedures to ensure that its approach to the application of customer due diligence measures does not result in the unjustified denial of access to financial services to clients acting lawfully. If the client is unable for legitimate and reasonable reasons to submit documents to verify his identity as prescribed in Article 7 of the AML Act, the service provider shall consider other ways to mitigate the ML/TF risk, including but not limited to:

a) determining the level and intensity of monitoring in a way that is proportionate to the ML/TF risk associated with the client, including the risk that a client who has not proven his identity in the manner prescribed in Article 7 of the AML Act may not be the person he claims to be;

b) only offer financial services that limit the ability of the client to misuse those services for the purpose of committing financial crimes. Such financial services may also make it easier for the service provider to identify unusual transactions or types of transactions, including unintentional use of the service. It is important, however, that any restrictions are proportionate and do not unduly or unnecessarily restrict clients' access to financial services.

40. In connection with the foregoing, the serve provider should also take into consideration the EBA Opinion on the application of customer due diligence measures to customers who are asylum seekers from higher-risk third countries or territories[6].

Beneficial owners

41. When fulfilling its obligations under Article 9(3) of the AML Act, the service provider is expected to satisfy at least the following requirements in order to understand the ownership and control structure of the client:

a) obtain and record in a retrievable form a written statement from the client as to the identity of its beneficial owners;

b) take all necessary and reasonable measures to verify the information; to this end, the service provider is expected to rely on the register of beneficial owners, if available.

Control exercised in other form

42. The measures taken by the service provider to understand the ownership and control structure of the client are expected to be sufficient for enabling the service provider to ascertain reasonably that it understands the risk associated with the different levels of ownership and control. In particular, the service provider is expected to ascertain that:

a) the ownership and control structure of the client is not unduly complex and difficult to understand; or

b) there is a legitimate legal or economic reason for the complex or non-transparent ownership and control structure.

43. The MNB expects the service provider to pay special attention to persons who exercise effective governance and control otherwise. Examples of “control exercised in other form” that the service provider should take into consideration include, but are not limited to:

a) control over the client without direct ownership, e.g. through close family ties or contractual relationships;

b) utilisation or use of or benefiting from assets owned by the client;

[6] This recommendation is governed by EBA opinion EBA-OP-2016-07.

c) responsibility for strategic decisions affecting the business practices or operations of the legal entity client.

44. The MNB expects the service provider to opt for not verifying the ownership structure of the customer only in the case of low risk exposure.

Identification of the client's senior executives

45. The MNB regards it as good practice for the service provider to accept the designated senior executive as the beneficial owner of the client only in the following cases:

a) the service provider has exhausted all possible means to identify the natural person who is the ultimate owner of the client or who otherwise exercises effective control over the client;

b) the fact that the service provider cannot identify the natural person ultimate owner of the client or who otherwise exercises effective governance or control over the client does not give rise to an undue suspicion of ML/TF; in particular, if it has ascertained that the reasons provided by the client for not being possible to identify the natural person ultimate owner of the client or who otherwise exercises effective governance or control over the client are acceptable.

46. The MNB regards it as good practice when in the cases mentioned in point 45, the service provider also records in a dedicated register the reason for identifying the senior executive as the beneficial owner instead of the client's beneficial owner.

Identifying the beneficial owner of a local government or state-owned company

47. If the client is a local government or state-owned company, the service provider should follow the steps in points 45 and 46 to identify the senior executive.

48. When identifying the beneficial owner of a local government or state-owned company, and in particular where the relationship is associated with an increased risk, for example because the local government or state-owned company originates from a country of higher ML/TF risk, the service provider should take measures on a risk-sensitive basis to determine whether the person it identifies as the beneficial owner has appropriate authorisation from the client to act on behalf of the client.

Proof of identity

49 The MNB expects the service provider when applying the provisions of Article 7 of the AML Act – in order to fulfil its customer due diligence obligations – to verify the identity of the client and, where applicable, of the beneficial owner, on the basis of reliable and independent information and data, regardless of the type of client identification – remote identification as defined in Article 17 of the AML Act, electronically (via a pre-audited electronic communication device) or based on documents presented in person – it used for obtaining such information.

50. The MNB expects the service provider to specify in its policies and procedures which information and data provided to it during customer due diligence it will regard as reliable and independent. In the course of this, the service provider should consider the following:

a) when assessing the reliability of the information:

i. the extent to which it was necessary to subject the client to certain checks in order to obtain the information or data provided;

ii. the official status, if any, of the person or institution performing these checks;

iii. the security level of the digital identification systems used; and

iv. how easily the information or data provided for identification purposes can be forged;

b) when assessing the independence of the information, the person or institution which originally published or made the data or information available:

i. to what extent it is connected to the client through direct personal, professional or family relationships; and

ii. whether it can be unduly influenced by the client.

The MNB is of the opinion that it is the information or data from central public administrations that the service provider may regard as substantially independent and reliable.

51. The MNB expects the service provider to assess the risks associated with each document submitted and the identification and verification method used, and to ensure that the method and type chosen is proportionate to the ML/TF risk associated with the client.

52. Where the initiation, establishment and maintenance of a business relationship or the execution of transaction orders is carried out remotely, the MNB expects the service provider, when performing its customer due diligence obligations, to:

a) take appropriate measures to ascertain that the customer is indeed the person he says he is; and

b) assess whether the remote nature of the relationship or transaction order increases the ML/TF risk and, if so, whether it is necessary to revise its customer due diligence measures accordingly. When assessing the risk associated with remote relationships, the service provider shall take into consideration the risk factors specified in Chapter III.2 hereof.

53. When a remote client relationship or transaction order is associated with increased risk, the service provider is expected to apply enhanced customer due diligence measures. In particular, the service provider should consider whether enhanced customer due diligence measures or a stepped-up procedure to verify the identity of the customer are justified.

54. In the MNB's view, the use of audited electronic communication devices alone does not increase the ML/TF risk, especially if they provide a high level of security within the meaning of Regulation 910/2014/EU[7].

Using innovative technological tools to verify the identity of the client

55. The MNB emphasises that the AML Act is technology-neutral, and thus it is up to the service provider to choose whether to use electronic means or documents or a combination of those to verify the identity of its clients. When using innovative technological tools to identify the client, the service provider is expected to ensure that this evidence is based on data or information from reliable and independent sources.

56. The MNB regards it as practice for the service provider to consider the following aspects as well when assessing the use of innovative technological tools:

a) infocommunication technology and security risks, in particular the risk that the innovative solution may be inappropriate, unreliable or easy to manipulate;

b) qualitative risks, in particular the risk that the sources of information used for verification purposes do not comply with the applicable statutory requirements in terms of their independence and reliability, and the risk that the scope of identity verification provided by the innovative solution is not proportionate to the level of ML/TF risk associated with the business relationship;

c) legal risks, in particular the risk that the third party providing the technological solution does not comply with applicable data protection legislation; and

d) the risk of identity theft (i.e. the risk that the client is not the person who he says he is or he is not a real person at all).

57. The MNB expects the service provider to define clearly the relationship it has with the third-party service provider providing the innovative solution. As part of this, the service provider is expected to specify the legal relationship underlying the connection (e.g. outsourcing contract or the case under Articles 22 and 23 of the AML Act) and to take the necessary steps to ascertain that the third party service provider providing the innovative solution:

a) has access and uses sufficient data from different sources and at different times, with special regard to the following elements:

[7] Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC

i. an electronic dataset based on the client's passport is not sufficient in remote situations without performing additional checks to ensure that the client is the person who he says he is and that the document has not been forged, and

ii. a single source of data or a single point in time is not sufficient to satisfy the verification standards in most situations;

b) under a contractual relationship, it shall comply with the obligations laid down in the agreement with the service provider and in the applicable national and EU legislation, and the third-party service provider providing the innovative solution shall forthwith inform the service provider of any change; and

c) its operation is transparent, and thus the service provider is always aware of the type of verifications performed, the sources used, the results obtained and the reliability of such results.

58. If the third-party service provider providing the innovative solution has its registered office, branch or business site in a third country, the service provider is expected to understand the legal and operational risks and data protection requirements arising from this circumstance and to mitigate these risks efficiently.

59. The MNB regards it as good practice for service providers to also take into consideration the ESA Joint Opinion of 2018 on the use of innovative solutions in the customer due diligence process[8], which contains further details in this regard.

Identification of the purpose and intended nature of the business relationship

60. The MNB regards it as good practice for the service provider, in order to determine the purpose and intended nature of the business relationship, to obtain information at least of the following:

a) the nature of the client's activities or business;

b) why the client chose the products and services of the service provider;

c) the amount and source of future cash flows on the account;

d) how the client will use the service provider's products and services;

e) whether the client has a business relationship with the service provider or, if the service provider is part of a group, with other members of the group, and how this affects the information obtained by service provider on the client; and

f) what qualifies as “usual” behaviour for that client or client category.

61. The MNB emphasises that the service provider should also take into consideration risk factors mentioned in points 16–19 hereof.

Simplified customer due diligence

62. The service provider may apply simplified customer due diligence to the extent permitted by the AML Act in situations where it assessed the ML/TF risk associated with the business relationship to be low.

63. Chapter IV of this recommendation specifies additional requirements for simplified customer due diligence measures.

Enhanced customer due diligence

64. With a view to managing and mitigating risks properly, the MNB considers it appropriate for the service provider to apply enhanced customer due diligence measures in higher risk situations. Enhanced customer due diligence measures must not be replaced by regular customer due diligence measures, but should be applied in addition to the regular customer due diligence measures.

[8] See ESA Joint Opinion JC 2017 81 of 23 January 2018.

Politically exposed persons

65. When in respect of the data on politically exposed persons the service provider uses a register other than the statutory official register of politically exposed persons, the MNB expects the service provider to ensure that the data in such registers are up-to-date and that it knows the limits of such lists. The service provider is expected to take further action, as necessary, for example in situations where filtering results are not convincing or do not meet the service provider's expectations.

66. Where the service provider has identified a client or the beneficial owner of the client as a politically exposed person, the MNB regards it as good practice for the service provider to:

a) Obtain the approval of the competent senior executives for any business relationship to be established or continued with politically exposed persons. The level of authority of the competent senior executive necessary for the approval should be aligned with the increased risk level of the business relationship. The manager approving a business relationship with a politically exposed person shall have sufficient governance and control authority to make informed decisions on issues that directly affect the risk profile of the service provider.

b) When considering whether to approve a relationship with a politically exposed person, the MNB deems it important that the manager should base his decision on the extent to which the establishment of the business relationship would expose the service provider to ML/TF risk and the extent to which the service provider is prepared to manage that risk effectively.

c) It shall apply a stepped-up procedure for the risk associated with transaction orders and business relationships. The service provider shall identify unusual transactions and regularly review the information available to it to ensure that it detects new or newly arising information that may affect the risk assessment in a timely manner. The frequency of enhanced monitoring should be determined by the high level of risk associated with the relationship.

67. The MNB expects the service provider to apply the aforementioned measures also to politically exposed persons, persons qualifying as a close relative of a politically exposed person or having close links to a politically exposed person, and regards it as good practice for the service provider to determine the scope of these measures based on risk sensitivity.

68. The MNB expects the service provider to ensure that the measures introduced by it to comply with the applicable law and this recommendation with regard to politically exposed persons do not result in the undue denial of access to financial services to clients qualifying as politically exposed persons.

High-risk third countries with strategic deficiencies

69. The MNB expects the service provider to assess the risks associated with business relationships and transactions if:

a) the client is known to have close personal or professional links with high-risk third countries with strategic deficiencies; or

b) the beneficial owner(s) is (are) known to have close personal or professional links with high-risk third countries with strategic deficiencies.

Correspondent banking relations

70. The service provider should apply measures specified in Chapter IV hereof with regard to the enhanced customer due diligence in relation to correspondent banking relationships.

Unusual transactions

71. Transactions show an unusual pattern, in particular if:

a) they are of a greater volume than the service provider would normally expect on the basis of its

knowledge of the client, the business relationship or the category of client;

b) are of an unusual or unexpected nature compared to the client's usual activities or the type of transactions associated with similar clients, products or services; or

c) are very complex compared to other similar transactions for similar types of clients, products or services, and the service provider is not aware of any reasonable economic justification or legitimate purpose or has doubts about the authenticity of the information provided by the client.

Other high-risk situations

72. The additional measures taken and the additional information requested as part of enhanced customer due diligence depend on why the service provider has classified the transaction or business relationship as high risk.

73. The MNB regards it as good practice for service providers to apply the following enhanced customer due diligence measures in addition to the measures specified in the AML Act:

a) Expanding the volume of information provided within the framework of customer due diligence:

i. Increasing the volume of information on the identity of the client or beneficial owner, the client's ownership or control structure to determine whether the service provider has a good understanding of the risk associated with the relationship. This may include obtaining and evaluating information about the reputation of the client or beneficial owner as well as assessing negative allegations concerning the client or beneficial owner (e.g. information about family members and close business associates; information about the past and present business activities of the client or beneficial owner; and seeking adverse media coverage).

ii. Obtaining information about the intended nature of the business relationship to determine whether the type and purpose of the business relationship is legitimate and to help the service provider prepare a full client risk profile. This may include obtaining the following information on: the number, amount and frequency of transactions made through the account, enabling the service provider to detect discrepancies that may lead to suspicions of money laundering (in certain cases, appropriate evidence may be requested).

iii. Clarifying the reasons why the client applies for a product or service in the respective country, in particular when the use of the product or service would be more justified in another country.

iv. Determining the destination of funds.

v. The nature of the client's or beneficial owner's business, in order to enable the service provider to understand better the true nature of the business relationship.

b) Improving the quality of information obtained for customer due diligence purposes to confirm the identity of the client or beneficial owner, including:

i. by requiring the first payment to be made from an account where it can be verified that is registered under the name of the client and held with a bank subject to customer due diligence standards at least as strict as those specified in the AML Act; or

ii. by establishing that the origin of the client's assets and funds used in the business relationship are not from criminal activity and that the source of the assets or funds is consistent with the service provider's information on the client and the nature of the business relationship. For certain client relationships of particularly high-risk, the only risk mitigation tool may be the verification of the source of assets and funds. The source of funds or assets can be verified by examining, among other things, VAT or personal income tax returns, copies of audited financial statements, payrolls, public documents or independent media reports.

c) Increasing the frequency of reviews to ensure that the service provider can continue to manage the risk associated with the individual business relationship or identify when the relationship is no longer consistent with the provider's risk appetite, and to help identify cases that require further review, including:

i. by increasing the frequency of reviewing the business relationship to determine whether the risk profile of the client has changed and whether the risk remained manageable;

ii. by the approval of a senior executive to establish or maintain a business relationship in order to understand the risk to which the service provider is exposed and to make an informed decision about the service provider's preparedness to manage that risk efficiently;

iii. by reviewing the business relationship more frequently to identify any changes in the client's risk profile and to take appropriate actions; or

iv. by the more frequent and in-depth monitoring of transactions to detect unusual or unexpected transactions that may give rise to suspicions of money laundering and terrorist financing. This may involve, among other things, exploring the purpose of funds or the underlying reason for certain transactions.

74. The MNB notes that Chapter IV of this recommendation lists additional enhanced customer due diligence measures that may be particularly relevant in the different sectors.

Keeping customer due diligence information up-to- date

75. The MNB expects the service provider upon implementing policies and procedures for keeping customer due diligence information up-to-date to pay special attention to the need of monitoring and recording information on clients on an ongoing basis to understand whether the level of risk associated with the business relationship has changed. The service provider should record the following information: an apparent change in the source of the client's funds, or a change in the client's ownership structure or behaviour that is consistently irreconcilable with the client profile available to the service provider.

76. In the event of any change in circumstances that increase the risk perceived in the client's profile, the service provider should apply customer due diligence measures in respect of the client. In such a case, the service provider does not necessarily need to apply all customer due diligence measures repeatedly, but rather to determine what additional measures should be applied in view of the increased risk. In cases of lower risk, the service provider may also rely, for example, on information obtained during the business relationship to update the customer due diligence information it possesses on the client.

III.4 Training

77. The MNB expects the service provider to draw the attention of its employees to the measures taken to comply with their obligations concerning the prevention of money laundering and terrorist financing during the preventive and annual internal training. As part of this, the service provider is expected to take steps to ensure that its employees acquire knowledge on the following:

a) internal risk assessment covering the entire activity, in accordance with Article 27(1) of the AML Act, and how it affects their daily work;

b) the content of policies and procedures for the prevention of money laundering and terrorist financing and how they are applied; and

c) the method of recognising suspicious or unusual transactions and activities and the internal procedures for taking actions related to those.

IV. Sector-specific guidelines

78. The sector-specific guidelines provide examples of the customer due diligence measures that credit institutions and financial service providers should apply on a risk-sensitive basis in high-risk and – to the extent permitted by the relevant legislation – low-risk situations. These examples are not exhaustive, and the credit institution and the financial service provider shall decide on the most appropriate customer due diligence measures in line with the level and type of the identified ML/TF risk.

79. The MNB expects credit institutions and financial service providers to apply also those sector-

specific guidelines that complement the general requirements applicable to all service providers, detailed in Chapter III of this recommendation. The sector-specific guidelines should be construed together with Chapter III and Annex 1. The sectoral risk factors to be taken into consideration are specified in Annex 1.

IV.1 Sector-specific guidelines for institutions providing correspondent banking services

80. For the definition of correspondent relations, primarily the provisions of point 23 of Article 3 of the AML Act should be taken into consideration.

81. In a correspondent banking relationship, the correspondent bank provides banking services to the bank using the correspondent banking services, either directly or on behalf of the clients of the bank using the services. The bank providing correspondent banking services usually has no business relationship with the clients of the bank using the services, and is usually not aware of their identity or the nature and purpose of the underlying transaction, unless this information is included in the payment order. The correspondent bank should consider the risk factors listed in Annex 1. The MNB regards it as good practice, after due consideration of the risk factors, to implement, among others, the following measures.

Measures

82. For the purposes of implementing Article 24/A (4) of the AML Act, the correspondent bank shall ascertain that the bank using the correspondent banking service does not permit the use of its account by a fictitious bank. As part of this, the MNB regards it as good practice for a correspondent bank to request confirmation from the bank using correspondent banking services that it is not doing business with fictitious banks, to request access to the rules and procedures of the bank using the services and it may take into consideration publicly available information, such as legal statements prohibiting the use of fictitious banks.

83. The MNB expects correspondent banks to bear in mind that usually it is not the explicit purpose of customer due diligence questionnaires provided by international organisations to support correspondent banks in complying with their obligations under the AML Act. With a view to complying with its obligations under the AML Act, the correspondent bank should assess whether the use of questionnaires is sufficient or additional measures should also be taken.

84. The MNB is of the opinion that there is no legal requirement for the correspondent bank to apply customer due diligence measures to individual clients of the respondent bank.

Non-EEA correspondent bank

85. If the bank using the correspondent banking service is located in a third country, the correspondent bank shall also apply the special enhanced customer due diligence measures prescribed in Article 24/A of the AML Act in addition to the customer due diligence measures specified in Articles 7–10 of the same.

86. With a view to implementing the measures prescribed by Article 24/A of the AML Act, the correspondent bank should take the following measures:

a) Collect sufficient information about the correspondent bank in order to understand the nature of the respondent bank's business in full to determine the extent to which the business activities of the bank using the service expose the correspondent bank to a higher risk of money laundering. As part of this, measures should be taken to understand the nature of the client base of the respondent bank, the type of activities that the bank using the service will perform through its correspondent bank account and to assess the risk associated with these activities.

b) Determine the reputation of the institution and the quality of supervision on the basis of publicly

available information. This means that the correspondent bank should consider the extent to which it relies on the fact that the bank using the correspondent banking services is subject to appropriate AML/CFT supervision. There are a number of publicly available sources (such as FATF or FSRB assessments) providing descriptions of effective supervision, which help correspondent banks in this.

c) Assessment of control mechanisms applied by the institution using the correspondent banking services for the prevention of ML/CFT. This means that the correspondent bank should carry out a qualitative assessment of the AML/CFT control framework of the bank using the correspondent banking services, and it is not enough merely to obtain a copy of the respondent bank's AML policies and procedures. This assessment should be recorded in a retrievable form. In accordance with the risk-based approach, where the risk is particularly high, and especially where the number of correspondent banking transactions is significant, the correspondent bank should consider on-site inspection and/or sample-based testing to ensure that the anti-money laundering policies and procedures of the bank using the correspondent banking services are effectively implemented.

d) Assess whether there is a need for approval by the senior executive of correspondent bank designated in the internal regulations pursuant to Article 65 of the AML Act prior to establishing new correspondent banking relationships and in cases where significant new risks arise, for example because the registered office of the institution using the correspondent banking services is in a country of higher ML/TF risk. The senior executive of the correspondent bank designated in point 35 of Article 3 AML Act should keep the governing body informed of correspondent banking relationships that pose a high risk and of the measures taken to manage that risk efficiently.

e) Defining the responsibilities of each institution. This may form part of the agreement between the correspondent bank and the bank using the correspondent banking service. The MNB regards it as good practice for the correspondent bank to lay down in writing, in a retrievable manner, the range of products and services provided to the bank using the service, who can use the correspondent banking service and how (for example, whether it can be used by other banks through their relationship with the bank using the service), and the AML/CFT responsibilities of the bank using the correspondent banking service. Where the risk associated with the relationship is high, it may be appropriate for the correspondent bank to verify – e.g. through subsequent transaction monitoring – that the bank using the correspondent banking service complies with its obligations under the agreement.

f) In the case of "payable through" accounts for the direct settlement of the client's own transactions on behalf of the bank and in the case of "nested account", the correspondent bank should ascertain whether the bank using the correspondent banking service has verified the identity of the clients with direct access to the correspondent's accounts and performed ongoing due diligence on them. The correspondent bank is also expected to ascertain that – upon request – it can provide the correspondent institution with the relevant customer due diligence data.

EEA correspondent bank

87. If the bank using the correspondent banking service is located in an EEA member state, the correspondent bank is expected to apply special customer due diligence measures based on risk sensitivity specified in Article 24/A of the AML Act.

88. If the risk associated with a bank using correspondent banking services in an EEA member state increases, the correspondent bank should apply special customer due diligence measures in accordance with Article 24/A of the AML Act. In this case, the correspondent bank should consider applying at least some of the enhanced customer due diligence measures described in Article 24/A of the AML Act.

IV.2 Sector-specific guidelines for institutions providing retail banking services

89. For the purposes of this recommendation, a retail bank is defined as a credit institution or

payment institution providing services to natural persons and small and medium-sized enterprises (hereinafter: retail bank). Examples of retail banking products and services include current accounts, mortgage loans, savings accounts, consumer and bridging loans and credit lines.

90. Retail banks are characterised by relatively easy access to products and services, and due to the nature of these products and services and the frequent transactions for large amount and business relationship, retail banking services can be involved in all stages of the terrorist financing and money laundering process. However, due to the volume of business relationships and transactions associated with retail banking services it may be particularly challenging to identify the ML/TF risk associated with the individual connections and to detect suspicious transactions.

91. In addition to the measures specified in Chapter III hereof, retail banks should also consider the sector-specific risk factors included in Annex 1 along with the following measures. The MNB regards it as good practice, after due consideration of the risk factors, to implement the following measures.

Measures

92. Where a retail bank uses automated systems to detect ML/TF risks associated with individual business relationships or transaction orders and to identify suspicious transactions, it is expected to ensure that these systems meet the criteria specified in the legislation and in this recommendation. The use of automated IT systems shall never replace the watchfulness of employees.

Enhanced customer due diligence

93. When the risks associated with a business relationship or transaction order increase, the retail bank should apply enhanced customer due diligence measures. These may include:

a) Verification of the identity of the client and the beneficial owner based on more than one reliable and independent source.

b) Identification and verification of other owners who are not the beneficial owners of the client or natural persons authorised to dispose over accounts, to give orders for transfers of funds or transfer of securities.

c) Creating a comprehensive client profile in order to obtain additional information about the client and the nature and purpose of the business relationship, for example by searching for open source or unfavourable media news or by ordering third party intelligence reports. Retail banks should seek to obtain, among others, the following information:

i. nature of the client's business or employment;

ii. the source of the funds involved in the client's business relationships, in order to ascertain their legitimacy;

iii. the purpose of the transaction, including, where applicable, the destination of the client's funds;

iv. other potential links of the client with other countries (registered office, operational facilities, branches, etc.) and individuals who may have an influence on its operations; and

v. if the client is located in another country, the reasons why the client tries to use retail banking services in another country.

d) Increasing the frequency of transaction monitoring.

e) More frequent review and, where necessary, updating of information and documents possessed by the retail bank. If the risk associated with the relationship is particularly high, retail banks should review the business relationship annually.

Simplified customer due diligence

Retail banks may apply simplified customer due diligence measures in low-risk cases specified in their internal regulations based on their own risk assessment defined in Article 65 of the AML Act.

Combined accounts

94. If the risk associated with the business relationship is low, the retail bank may apply simplified customer due diligence measures. The MNB regards it as good practice for a retail bank to consider a business relationship to be of low risk in respect of combined accounts in the following cases:

a) The client is subject to AML/CFT obligation in an EEA State or a third country the AML/TF regime of which is at least as strict as the requirements of the AML Act and is subject to effective supervision in terms of compliance with those.

b) The client is an obliged service provider subject to AML/CFT obligations in another EEA State rather than being an undertaking, and it is subject to efficient supervision in terms of compliance with these requirements.

c) Based on the assessment performed by the retail bank concerning the business activity of the client, the types of customers served by the client as part of its business activity and the assessment of the countries affecting the client's business activity, in addition to other considerations, the ML/TF risk associated with the business relationship is low.

d) The retail bank is convinced that the client applies strict and risk-sensitive customer due diligence measures in relation to its own customers and the beneficial owners of its own customers (it may be appropriate for the retail bank to put in place risk-sensitive measures to assess whether the client's customer due diligence policies and procedures are adequate, e.g. through direct contact with the client).

e) The retail bank applied risk-sensitive measures to ensure that – upon request – the client promptly provides customer due diligence information and documents relating to the underlying clients, i.e. the beneficial owners of funds held on the combined account, for example by including provisions to this effect in the contract with the client or by verifying, by sampling, that the client is able to provide customer due diligence information upon request.

Clients offering services related to virtual currencies

95. The MNB reminds retail banks to the fact that, although service providers offering exchange services between virtual currencies and legal tender, virtual currency exchange services and custodial wallet providers are service providers falling within the AML Act, the issuance or holding of virtual currencies as defined in point 47 of Article Section 3 of the AML Act is currently largely unregulated in the European Union, which increases ML/TF risks.[9]

96. When establishing a business relationship with a client providing virtual currency services, the retail bank should consider the ML/TF risk associated with virtual currencies as part of its assessment of the ML/TF risk connected to the client.

97. The retail bank should treat the following businesses, among others, as high-risk clients in relation to virtual currencies:

a) operating as a virtual currency trading platform, which carries out exchange between legal tenders and virtual currencies;

b) operating as a virtual currency trading platform, which carries out exchange between virtual currencies;

c) operating as a virtual currency trading platform that allows peer-to-peer transactions;

d) providing custodial wallet services;

e) organising, advising or realising profit on "Initial Coin Offering" (hereinafter: ICO).

98. In order to ensure that the level of ML/TF risk connected to clients offering virtual currency services remains moderate, in their case the MNB does not regard it as good practice to apply

[9] In this context, the MNB draws the attention of banks to the EBA's report of 9 January 2019 on crypto-assets and the Proposal for a regulation on Markets of Crypto-assets (MiCA) as part of the European Commission's new digital finance package.

simplified customer due diligence measures.

99. For the purposes of implementing customer due diligence measures, the retail bank should take at least the following measures:

a) it should initiate a dialogue with the client through direct contact to understand the nature of the business and the ML/TF risks posed by the business activity;

b) in addition to verifying the identity of the beneficial owners of the client, the due diligence of the client's senior executive – as long as he is not identical with the beneficial owner – should be also performed, also taking into consideration any adverse information;

c) it should be identified to what extent these clients apply their own customer due diligence measures to their customers, either based on a statutory obligation or on a voluntary basis;

d) it should be determined whether the client is registered or authorised in an EEA Member State or in a third country and the adequacy of the respective third country's ML/TF regime should be assessed; and

e) it should find out whether the companies using ICOs to raise money in the form of virtual currencies are legally established and, where applicable, regulated.

100. Where such clients are associated with increased risk, the retail bank should apply enhanced client due diligence measures in accordance with Chapter III hereof.

IV.3 Sector-specific guidelines for electronic money institutions

101. This recommendation provides guidelines for electronic money institutions specified in point 28d) of Article 3 of the AML Act (hereinafter: electronic money institutions). The level of ML/TF risk associated with electronic money depends primarily on the characteristics of the individual electronic money products and the extent to which electronic money institutions use other persons to sell and redeem electronic money on their behalf. In addition to the measures specified in Chapter III hereof, electronic money institutions should also consider the sector-specific risk factors included in Annex 1 along with the following measures.

Measures

102. Electronic money institutions should apply the customer due diligence measures under Article 24/C of the AML Act.

103. Regardless of the level of risk, the electronic money institution should obtain sufficient information about its clients or the types of clients targeted by its product to facilitate the performance of substantive ongoing monitoring of the business relationship. With regard to the filtering and monitoring systems to be used by electronic money institutions, the MNB expects that those should:

(a) detect unusual transactions or suspicious patterns of behaviour, including unexpected use of the product in a way other than intended, and it should make it possible for the electronic money institution to disable the product manually or via chip until it is satisfied that there is no reason for suspicion;

b) identify discrepancies between the information provided and the information perceived, for example between the country of origin information provided and the IP address detected electronically;

c) compare data on other business relations with data possessed by the electronic money institution, which can identify patterns such as the same funding instrument or the same contact details;

d) identify if the product is used by traders in goods and services that carry a high risk of financial crime;

e) link electronic money products to devices or, in the case of web-based transactions, to IP addresses.

Enhanced customer due diligence

104. In order to comply with the requirements in respect of relationships or transactions involving high-risk third countries with strategic deficiencies, the electronic money institution should apply enhanced customer due diligence measures as specified in subsection III.3 of Chapter III *(Customer due diligence measures*).

105. Enhanced customer due diligence measures applicable in high-risk situations:

a) obtaining additional information on the client during customer due diligence, for example on the source of funds;

b) using additional verification measures from a wider range of reliable and independent sources (e.g. comparison with online databases) to verify the identity of the client or beneficial owner;

c) obtaining additional information about the intended nature of the business relationship, such as asking clients about their business activities and the countries to which they intend to transfer electronic money;

d) obtaining information on the merchant/beneficiary, in particular where the electronic money institution has a good reason to believe that its products are being used for purchasing illegal or age-restricted goods;

e) identity verification to prevent fraud;

f) applying an enhanced procedure for the client relationship and individual transactions;

g) identifying the source and destination of funds.

Simplified customer due diligence

106. The MNB does not support the use of simplified due diligence measures beyond the cases prescribed Article 24/C (1) and (2) of the AML Act.

IV.4 Sector-specific guidelines for institutions providing money transfer services

107. Money transfer providers are payment institutions, electronic money institutions or credit institutions authorised to provide funds transfer services under point 87 *f)* of Article 6(1) of the Credit Institutions Act (hereinafter: money transfer institution).

108. Money transfer is a payment service, defined in point 54 of Article 6(1) of the Credit Institutions Act, which is based on cash provided by the payer to the payment service provider, which is transferred by the sender service provider – for example via a communication network – to the beneficiary or to another payment service provider acting on behalf of the beneficiary in order to pay the money to the beneficiary. Since many money transfer providers perform primarily transaction-based activity, money transfer providers should give consideration to the type of monitoring systems and controls they use for detecting ML/TF attempts, even if they have only basic or no customer due diligence information on the client, as no business relationship has been established with the client.

109. Some money transfer providers use payment intermediaries for the provision of payment services on their behalf. Payment intermediaries often provide payment services as a complementary service to their core business and are not necessarily obliged service providers falling within the ML/TF legislation, and accordingly, their expertise in AML/CFT may be limited.

110. Money transfer activity may expose the money transfer service provider to ML/TF risk due to the simplicity and speed of transactions, its global scope and often cash-based nature. In addition, due to the nature of such payment services, the money transfer service provider often only executes transaction orders and does not establish any business relationship with its clients, which means that it may have limited knowledge of the ML/TF risk associated with the client. Bearing this in mind, in addition to the risk factors and measures specified in Chapter III hereof, money transfer providers should also consider the sector-specific risk factors included in Annex 1 along with the following measures. A money transfer service provider whose licence covers business activities such as the

provision of payment initiation services and account information services should also take into consideration the sector-specific guidelines for providers of payment initiation services and account information services specified in subtitle IV.9 of this recommendation.

Measures

111. Since the business activity of many money transfer service providers is primarily transaction-based, money transfer providers should give consideration as to the type of monitoring systems and controls to be implemented to ensure that ML/TF attempts are detected even if it has only basic or no customer due diligence information on the client because no business relationship has been established. When analysing the appropriate monitoring systems, the MNB expects the money transfer service provider to ensure that they are consistent with the volume and complexity of its business activity and the volume of transactions.

112. The service provider should implement the following:

a) systems for identifying a series of related transaction orders, including transactions that may qualify as a business relationship under the money transfer provider's policies and procedures (e.g. systems that identify series of transactions below EUR 1,000 where the payer and the beneficiary are the same and have an element of continuance);

b) systems that detect when the beneficiary of different clients' transactions is the same;

c) systems that facilitate the identification of the source and destination of funds;

d) systems that facilitate full traceability of the transactions as well as the number of economic agents involved in the payment chain;

e) systems to detect whether the transfer is to or from a high-risk third country with strategic deficiencies; and

f) systems that ensure that only persons authorised to provide money transfer services participate in the payment chain.

Use of payment service intermediaries

113. The MNB expects money transfer providers relying on a payment intermediary to provide money transfer services to know the payment intermediary it has engaged. As part of this, the money transfer service provider should develop and maintain appropriate and risk-sensitive policies and procedures to reduce the risk of payment intermediaries being involved or used in ML/TF activities. To this end the following measures should be taken:

a) Where the payment intermediary is a legal entity, identification of its owner or controlling entity to ensure that the money transfer service provider can ascertain that the use of the payment intermediary does not increase the money transfer provider’s ML/TF risk.

b) In accordance with the requirements of Article 55(3)*i)* of Act CCXXXV of 2013 on certain payment service providers, obtaining evidence that the management and other persons responsible for the management of the payment intermediary are fit to perform their duties, with special regard to fairness, integrity and good repute. The assessment carried out by the money transfer provider is expected to be proportionate to the nature, complexity and magnitude of the ML/TF risk inherent in the payment services provided by the payment intermediary, which may be based on the money transfer provider's customer due diligence procedures.

c) Taking appropriate measures to ensure that the payment intermediary's internal AML/CFT controls remain adequate throughout the duration of the intermediary relationship, e.g. by reviewing a sample of the payment intermediary's transactions or by carrying out on-site inspections of the payment intermediary's control mechanisms. Where the payment intermediary's internal AML/CFT control mechanism differ from those of the money transfer service provider, for example because the payment intermediary represents more than one payer or because the agent itself is a service provider under AML/CFT legislation, the money transfer service provider should evaluate and manage the risk

that these differences may affect its own or the payment intermediary's AML/CFT compliance.

d) Providing payment intermediaries with AML/CFT training to ensure that payment intermediaries are adequately aware of the relevant ML/TF risks and the quality of AML/CFT control mechanisms that the money transfer service provider expects of them.

IV.5 Sector-specific guidelines for institutions providing asset management services

114. For the purposes of this recommendation, asset management is the provision of banking and other financial services to affluent individuals and their families or businesses. Asset management is also known as private banking, fiduciary services (hereinafter institutions providing such services: asset management service providers). The asset management service provider's clients are supported by relationship managers offering personalised services.

115. Due to a number of specific characteristics of asset management, it implies a higher risk of money laundering compared to the risk typically associated with retail banking. According to the MNB's assessment, the services of an asset management service provider may be particularly vulnerable to misuse by clients who wish to conceal the source of their funds or, for example, to avoid tax in their jurisdiction. In view of this, in addition to the measures specified in Chapter III hereof, asset management service providers should also consider the sector-specific risk factors included in Annex 1 along with the following measures. In connection with this, the sector-specific guidelines for retail banks, for institutions providing life insurance services and for investment fund managers included in subtitles IV.2, IV.6 and IV.7 of this recommendation may also be relevant.

Measures

116. The employee (relationship manager) who manages the relationship with the client of the asset management service provider has a key role in risk assessment. The relationship manager's close contact with the client facilitates the gathering of information that may help obtain a more complete picture of the purpose and nature of the client's business (for example, the source of the client's funds, why some complex or unusual arrangements may still be real and legitimate, or why additional collateral may be required). However, this close relationship may also lead to a conflict of interest if the relationship manager becomes too close to the client, and thus it may jeopardise the efforts of the asset management service provider to manage the risk of financial crime. Consequently, it may also be necessary to perform an independent review of the risk assessment, for example by the compliance area and senior executives.

117. In order to implement Article 13(7) of the AML Act, the MNB expects that asset management service provider – when the beneficiaries of the fiduciary asset management have been identified by reference to a category of beneficiaries – to obtain sufficient information to ascertain that it will be possible to determine the identity of the beneficiaries at the time of payment or when the beneficiaries exercise their rights.

Enhanced customer due diligence

118. In high-risk situations, the following enhanced customer due diligence measures may be necessary. Obtaining and verifying additional information on clients compared to normal risk situations, and regularly reviewing and updating this information to reflect material changes in the client's profile. The asset management service provider shall perform reviews based on risk sensitivity and clients representing higher risk should be reviewed at least once a year, or even more often if necessary. The MNB regards it as good practice for these procedures to include the recording of visits to clients' premises, whether in their home or in their business premises, including any changes in the client profile or other information that may affect the risk assessment carried out following such visits, considering the following aspects:

a) Identifying the source of assets and funds. When the risk is particularly high or when the asset management service provider has doubts about the legitimate origin of funds, the appropriate risk mitigation tool may be to verify the source of assets and funds. Among others, the following items may serve the verification of the source of the assets or funds: original or certified copy of the most recent pay slip; written confirmation of annual salary signed by the employer; original or certified copy of a sales contract for an investment or business; certificate of sale countersigned by a lawyer; original or certified copy of a will or grant of probate; certificate of inheritance signed by a lawyer, trustee or executor; web search of the business register to confirm the sale of a business.

b) Determining the destination of funds.

c) More rigorous scrutiny and due diligence of business relationships than usual upon the provision of general financial services, such as retail banking or investment management.

d) Independent internal review and, where necessary, seeking the approval of the asset manager's senior executive for new and existing clients based on risk sensitivity.

e) Continuous monitoring of transactions, including real-time review of certain transactions to detect unusual or suspicious activity. This may include measures to determine whether any of the following falls outside the business risk profile: credit transfers (transfer of cash, investments or other instruments); bank transfers; significant changes in activity; transactions involving countries representing higher ML/TF risk.

119. Monitoring measures may include the use of thresholds and an investigation procedure whereby the customer relationship managers or (subject to reaching a certain threshold) the compliance area or senior executives can immediately investigate unusual behaviour.

a) Monitoring of public reports or other sources of news to obtain information about the client or persons closely associated with the client, companies, potential acquisition targets or third party beneficiaries to whom the client makes payments.

b) Ensuring that cash or other physical valuables (e.g. holiday cheques) are handled only by the cash desks of the asset management service provider, without the involvement of the customer relationship managers, if possible.

c) Ensuring that the asset management service provider can ascertain that the use of complex business structures – such as fiduciary asset management and private investment vehicles – by the client has a legitimate and genuine purpose and that the identity of the ultimate beneficial owner is known.

Simplified customer due diligence

120. The MNB does not recommend the use of simplified customer due diligence for asset management.

IV.6 Sector-specific guidelines for trade finance

121. Trade finance is the management of payments to facilitate the movement of goods (and the provision of services) inland or across borders. In international trade, the risk for the importer is that the goods do not arrive, while the risk for the exporter is that the goods are not paid for. With a view to mitigating these risks, many trade finance instruments place credit institutions and financial service providers (for the purposes of this chapter, institutions providing such services hereinafter: trade finance providers) in the centre of the transaction.

122. Trade finance can take many different forms. Among others:

a) "Open account" transactions: transactions where the buyer makes payment after receiving the goods. These are the most common means of trade finance, but the underlying commercial nature of the transaction is often not known to the credit institutions that make the funds transfer. To manage the risks associated with such transactions, banks should set out from the provisions of Chapter III of this recommendation.

b) Documentary credit (letter of credit): a letter of credit is a financial instrument issued by a bank that guarantees payment to a named beneficiary (typically an exporter) on presentation of certain "appropriate" documents (such as proof of shipment of goods) specified in the credit terms.

c) Documentary collection: documentary collection refers to the process whereby a "collecting" bank collects a payment or accepted bill of exchange from importers of goods for the purpose of forwarding the payment to exporters. In return, the collecting bank provides the importer with the relevant commercial documents (received from the exporter, usually via its bank).

123. Other financing products, such as factoring, forfeiting or structured finance, or broader activities similar to project finance, fall outside the scope of this recommendation. A trade finance provider offering such products should follow the general guidance in Chapter III of this recommendation, in view of the fact that trade finance instruments can be misused for ML/TF purposes (for example, the buyer and seller may collaborate in providing false information on the price, quality or volume of goods for the purpose of an international transfer of money or value).

124. The International Chamber of Commerce developed standards for the use of letters of credit and documentary collections, but these do not address issues related to financial crime. The MNB warns trade finance providers that the application of the standards does not mean that credit institutions do not need to comply with their AML/CFT obligations.

125. In addition to the measures specified in Chapter III hereof, trade finance providers should also consider the sector-specific risk factors listed in Annex 1 along with the following measures.

126. A trade finance provider involved in a trade finance transaction often has access to only partial information about the transaction and the parties to it. Commercial documents can be diverse and trade finance providers may not have specialised knowledge of the different types of commercial documents they receive. This may complicate the identification and assessment of ML/TF risks. However, the trade finance service provider must use sound judgement and professional assessment for deciding to what extent the information and documents in its possession may give rise to ML/TF concerns or suspicions.

Measures

127. The MNB expects the trade finance service provider to carry out the statutory customer due diligence measures in respect of the ordering party. In practice, the majority of trade finance providers only accept instructions from existing clients, and the trade finance provider's wider business relationship with the client may ease due diligence efforts.

128. As part of the customer due diligence process, the trade finance provider should take steps to learn about its client's business activities. For example, the trade finance provider may obtain information on: the countries the client trades with, the trade routes it uses, the goods it trades in, the entities it does business with (e.g. customers, suppliers), whether it relies on agents or third parties and if yes, the location of those. This may help the trade finance provider find out more about the clients and identify unusual or suspicious transactions.

129. If the credit institution is a correspondent bank, the bank that uses the correspondent banking service shall be subjected to due diligence. Correspondent banks should follow the sector-specific guidelines in subtitle IV.1 of this recommendation.

Enhanced customer due diligence

130. In situations of higher risk, the trade finance provider should apply enhanced customer due diligence. As part of this, the trade finance provider should consider whether more thorough due diligence verifications of the transaction and of other parties involved in the transaction (including parties other than clients) are necessary.

131. Verification of other parties involved in the transaction may include:

a) Steps to understand better the ownership structure and background of the other actors involved

in the transaction, especially if they are located in a country of higher ML/TF risk or if they handle high-risk goods. This may include the verification of company registers and third party news sources, or searching the internet for open sources.

b) Obtaining additional information on the financial standing of the parties involved.

132. Verification of transactions may include:

a) the use of third party or open source data sources, –such as International Maritime Bureau data sources (e.g. warning records, bills of lading, freight and pricing audits) – or using free container tracking services provided by shipping companies to verify the information provided and to check that the purpose of the transaction is legitimate;

b) assessing, based on professional judgement, whether the pricing of goods is commercially reasonable, in particular for traded goods for which reliable and up-to-date pricing information can be obtained;

c) verifying that the weight and volume of the transported goods are in accordance with the mode of transport.

133. As the vast majority of letters of credit and documentary collections are paper-based and accompanied by commercial documents (such as invoices, bills of lading and manifests), automated monitoring of transactions may not be feasible. The trade finance service provider performing the processing should evaluate these documents in terms of their consistency with the conditions of the commercial transaction and prescribe for its staff to use their expertise and professional judgement to consider whether any unusual features may warrant enhanced customer due diligence measures or any suspicion of ML/TF arises.

Simplified customer due diligence

134. Routine checks carried out by trade finance service providers to detect fraud and ensure that transactions comply with the standards set by the International Chamber of Commerce mean that in practice, even in situations involving lower risk, simplified customer due diligence measures must not be applied, and accordingly the MNB does not deem it sufficient to carry out simplified customer due diligence.

IV.7 Sector-specific guidelines for institutions providing life insurance services

The purpose of life insurance is to provide financial protection for the beneficiary against the risk of draining savings during the years of retirement due to an uncertain future event, such as death, illness or longer life expectancy (longevity risk). The protection is provided by an insurer who pools the financial risks for several different policyholders. Life insurance can be purchased as an investment product or for retirement purposes, and the savings component and risk cover may also be purchased in a single contract (either as a unit-linked or traditional life insurance product). Due to the nature of the insurance risk, the group of pure risk life insurances – where there is no savings/investment part of the contract – is also very important. In the case of this latter product type the risk of money laundering is also very low. There are single premium and regular premium life insurance policies, and in the case of contracts with a savings component, the client usually also has the option to pay top-up premium in addition to the regular premium agreed.

135. Life insurance is sold through various distribution channels to clients, who may be natural persons, legal entities or unincorporated undertakings. The beneficiary of the contract may be the policyholder or a named or designated third party. The beneficiary may change during the term and the original beneficiary may never receive the life insurance benefit.

136. The majority of life insurance policies with a savings component are designed for long term and usually the payment of insurance benefit is subject to a defined, documented insured event specified in the contract, such as death or retirement. This means that many life insurance policies are not flexible enough to be the first choice of money launderers. However, similar to other financial

services products, it may happen – but here as a lower risk than the average – that the funds used for buying life insurance come from crime.

137. In addition to the measures specified in Chapter III hereof, life insurance providers should also consider the sector-specific risk factors listed in Annex 1 along with the following measures. The sector-specific requirements for asset management and for investment fund service providers described in subtitles IV.5 and IV.8 of this recommendation may also be relevant. Upon relying on intermediaries, the relevant risk factors are those related to the distribution channel. This guideline may also be useful for intermediaries.

Measures

138. Article 13(3)-(4) of the AML Act prescribe with regard to the life insurance business that the provider of life insurance services must apply customer due diligence measures not only in respect of the client and the beneficial owner, but also in respect of the beneficiaries immediately after the identification or designation of the beneficiaries. This means that the provider of life insurance services should:

a) obtain the name of the beneficiary where the client specifies a natural person, legal entity or an unincorporated enterprise as beneficiary; or

b) obtain sufficient information for establishing the identity of the beneficiaries at the time of payment, where the client specifies the beneficiaries as a group of persons or on the basis of certain characteristics. For example, if the beneficiaries are “my future grandchildren”, the insurer should obtain information about the policyholder's children;

c) verify that payments of the insurance amounts are actually made to the beneficiaries indicated in the insurance policy already subjected to due diligence. The recipients of payments of insurance amounts should always be considered as beneficiaries for the purposes of prevention of money laundering, regardless of whether they are identified as such in the insurance policy;

d) the provider of life insurance services shall verify the identity of the beneficiaries at the time of payment, at the latest. If the provider of life insurance services knows that the life insurance policy has been assigned to a third party and that this third party will receive the policy amount, it shall identify the beneficial owner at the time of the assignment.

Enhanced customer due diligence

In high-risk situations, the following enhanced customer due diligence measures may be necessary:

139. If the client makes use of the free termination /cancellation period, the premium shall be refunded to the bank account of the client from which the money was paid. The provider of life insurance services should verify the identity of the client before refunding, especially if the premium is high or the circumstances appear unusual otherwise. The provider of life insurance services should also check whether the cancellation raises suspicions of money laundering and whether it needs to report suspicious activity.

140. Further steps can be taken to ensure that the provider of life insurance services has broader knowledge of the client, the beneficial owner, the beneficiary or the beneficial owner of the beneficiary, third party payers and beneficiaries. These may include, for example, the following measures:

a) refraining from the application of Article 13 (2) of the AML Act providing exemption from preliminary customer due diligence;

b) verification of the identity of other relevant parties, including third-party payers and beneficiaries, before the start of the business relationship;

c) obtaining additional information on the purpose and nature of the intended business relationship;

d) obtaining additional information on the client;

e) more frequent review of the identification data of the client and the beneficial owner;

f) if the payer differs from the client, clarifying the reason for the difference;

g) verification of their identity based on more than one reliable and independent source;

h) obtaining data concerning the source of the client's funds, such as employment and salary, probate or divorce settlements;

i) where possible, identifying the beneficiary at the start of the business relationship, rather than identifying or naming him later, bearing in mind the possibility that the beneficiary may change during the period of insurance;

j) identification and verification of the identity of the beneficial owner;

k) taking measures in accordance with the provisions of Articles 9/A and 9/B of the AML Act to determine whether the client is a politically exposed person and whether the beneficiary or the beneficial owner of the beneficiary is a politically exposed person at the time of the full or partial assignment of the policy or upon payment, at the latest; and

l) prescribing that the first payment should be made from an account held under the customer's name with a bank that is subject to customer due diligence standards at least as strict as those prescribed by the AML Act.

141. Article 16 (1)*d)* of the AML Act prescribes that in the case of business relations with politically exposed persons, the provider of life insurance services shall apply not only the customer due diligence measures under Articles 7–10 of the AML Act, but also perform enhanced customer due diligence for the entire business relationship; furthermore, pursuant to Article 10(3) of the AML Act, prior to making payment under the policy the provider of life insurance services should also inform its senior executives in order to enable them to form an informed opinion on the ML/TF risk associated with the situation and to decide on the most appropriate measures to mitigate the risk.

142. Furthermore, providers of life insurance services should:

a) obtain additional information on the business relationship in order to understand the nature of the relationship between the client or the insured and the beneficiary, and the nature of the relationship between the payer and the beneficiary where the payer is a person other than the client or the insured; and

b) enhance the verification of the source of funds.

143. If the beneficiary is a politically exposed person, the MNB expects the providers of life insurance services to perform the enhanced customer due diligence well before the payment of the insurance benefit under the policy.

144. Transactions may need to be monitored more frequently and more thoroughly, including, if necessary, obtaining information on the source of funds.

Simplified customer due diligence

145. Simplified customer due diligence measures may be applied in low-risk situations. The MNB considers the following cases to be of low risk:

a) When the payment is made from an account held in the name of or jointly owned with the policyholder at a supervised credit institution in an EEA country and the provider of life insurance services has ascertained this.

b) When the payment to the beneficiary is made to an account held with a supervised credit institution in an EEA country, the MNB is of the opinion that it can be assumed that the identity of the beneficiary of the insurance has been verified.

IV.8 Sector-specific guidelines for institutions performing investment services activity

146. Upon providing the investment services stipulated in Article 5(1) of Act CXXXVIII of 2007 on Investment Firms and Commodity Dealers, and on the Regulations Governing their Activities

(hereinafter: Investment Firms Act), investment firms defined in point 10 of Article 4(2) of the Investment Firms Act should take into consideration, in addition to the factors specified in Chapter III of this recommendation, the sector-specific risk factors listed in Annex 1 along with the measures specified below, and the sector-specific guidance for institutions providing asset management services described in subtitle IV.5 may also be relevant to them.

147. Investment management is the management of an investor's assets to achieve specific investment objectives. It includes both discretionary investment management, where investment managers make investment decisions on behalf of their clients, and advisory investment management, where investment managers advise their clients on the types of investments they recommend, but do not execute transactions on behalf of their clients.

148. An investment firm usually has a limited number of private or institutional clients, many of whom are wealthy, such as affluent private individuals, fiduciaries, corporations, government agencies and other investors. Client funds are often managed by a local custodian rather than by the investment firm. Investment firms should take into consideration that ML/TF risk in this sector is primarily triggered by the risk associated with the clients served by the investment firm. Furthermore, due to the nature of the activities carried out by the investment firm, investment firms may be exposed to predicate crime similar to market abuse, which may give rise to ML/TF risk.

Measures

149. Investment firms are expected to know their clients thoroughly in order to help them identify the right investment portfolios. For this purpose, the investment service provider collects information similar to that it also obtains for AML/CFT purposes. Investment firms should consider the extent to which the information thus obtained can also be used for fulfilling their general customer due diligence obligations. In situations of higher risk, investment firms should take the enhanced client due diligence measures specified in Chapter III of this recommendation.

150. The MNB expects investment firms to identify and, where necessary, verify the identity of their clients' underlying investors when the client is a third-party non-regulated investor.

151. Investment firms should find out reason for payments or transfers made to or by unverified third parties.

IV.9 Sector-specific guidelines for institutions performing investment fund management activity

152. Pursuant to Article 3(28)*I)* of the AML Act, the requirements specified in this subtitle apply to the investment fund managers' activity of distributing mutual fund shares and the activity specified in the Investment Firms Act.

153. The type and number of parties involved in the process of distributing a fund's mutual fund shares depends, among other things, on the nature of the fund and it may affect the volume of information known by the fund manager distributing the mutual fund shares about its client and its investors. Responsibility for compliance with AML/CFT obligations lies with the fund manager distributing the mutual fund shares, due to the fact that investment funds fall outside the scope of the AML Act.

154. Investment funds may be used by natural persons or organisations for ML/TF purposes:

a) Retail funds are often distributed without personal presence; such funds often can be accessed easily and relatively quickly and shares in such funds are transferable between different parties.

b) Despite the often medium to long-term nature of such investments – due to which these products are less attractive for money laundering purposes – their growth and capacity to generate income may still raise the interest of money launderers.

155. Other parties involved in the distribution of the fund's mutual fund shares, such as intermediaries, should also comply with their own customer due diligence requirements and, where

applicable, they should also apply the relevant subtitles of this recommendation. In addition to the measures specified in Chapter III hereof, investment fund manager institutions should also consider the sector-specific risk factors listed in Annex 1 along with the following measures.

Measures

156. In addition to the enhanced customer due diligence prescribed by the AML Act, in high-risk situations investment fund managers distributing the mutual fund shares should prescribe that the first payment is made from an account registered under the name of or owned jointly by the client held with a supervised credit institution or financial service provider in an EEA country or with a supervised credit institution or financial service provider in a third country where the AML/CFT requirements are at least as strict as those of the AML Act.

157. In situations of lower risk, to the extent permitted by law, and where funds are verifiably transferred to or from an account registered under the name of or jointly owned by the client, held with a supervised credit institution or financial service provider in an EEA country, the investment fund managers distributing the mutual fund shares may, for example, use the source of funds as a simplified customer due diligence measure to comply with certain customer due diligence measures.

158. In situations of higher risk, where the financial intermediary is a client of the investment fund manager, the fund manager should apply customer due diligence measures in respect of the financial intermediary based on risk sensitivity. The investment fund manager should also take measures based on risk sensitivity both for the identification and verification of the identity of the financial intermediary’s underlying investors, as these investors are the beneficial owners of the funds invested through the intermediary. In situations of low risk, fund managers may apply simplified customer due diligence measures to the extent permitted by law. The low risk level is substantiated by the following factors:

a) The financial intermediary is subject to AML/CFT obligations in an EEA country or in a third country where the AML/CFT requirements are at least as strict as those of the AML Act.

b) The financial intermediary is efficiently supervised in respect of compliance with these requirements.

c) The investment fund manager took steps based on risk sensitivity to ascertain that the ML/TF risk associated with the business relationship is low, based on, among others, the assessment of the financial intermediary's business activity, the types of clients served by the intermediary's business and the countries affecting the business activity of the intermediary.

d) The investment fund manager took steps based on risk sensitivity to ascertain that the intermediary applies strict and risk-sensitive customer due diligence measures in relation to its own clients and the beneficial owners of its clients. As part of this, the investment fund manager assesses the adequacy of the intermediary's customer due diligence policies and procedures based on risk sensitivity, for example based on publicly available historical data on the intermediary's compliance or by direct communication with the intermediary.

e) The investment fund manager took steps based on risk sensitivity to ascertain that upon request the intermediary would promptly provide customer due diligence information and documents relating to the underlying investors, for example by including the relevant provisions in the contract with the intermediary or verifying by sampling the intermediary's ability to provide customer due diligence information on request.

159. In the case of increased risk, enhanced customer due diligence measures should be applied, which may include the customer due diligence measures detailed below.

a) The investment fund manager should apply customer due diligence measures in respect of the ultimate investor based on risk sensitivity. The investment fund manager may rely on the results of the customer due diligence carried out by another service provider in order to fulfil its customer due diligence obligations, in accordance with and subject to the conditions specified in Articles 22 and 23 of the AML Act.

b) In situations of low risk, investment fund managers may apply simplified customer due diligence measures to the extent permitted by law. If the conditions listed in the foregoing are satisfied, the investment fund manager may accept identification data as part of the simplified customer due diligence measures as defined in Article 23(1) of the AML Act; the investment fund manager should obtain such data from the other service provider performing the customer due diligence by a reasonable deadline. The investment fund manager should determine such deadline applying a risk-based approach.

IV.10 Sector-specific guidelines for providers of payment initiation and account information services

160. Providers of payment initiation services and account information services should take into consideration that although pursuant to subpoint *g)* and *h)* of point 87 of Article 6(1) of the Credit Institutions Act providers of payment initiation services and providers of account information services, respectively, are obliged service providers falling within the AML Act, the ML/TF risk associated with them is limited due to the following factors:

a) although the providers of payment initiation services participate in payment chain, they do not execute payment transactions and do not hold the funds of the users of payment services;

*b)*the providers of account information services do not participate in the payment chain and do not hold the funds of payment service users.

161. In addition to the measures specified in Chapter III hereof, providers of payment initiation service or account information services should also consider the sector-specific risk factors listed in Annex 1 along with the following measures.

Measures

162. Providers of payment initiation services or account information services shall take appropriate measures to identify and assess the ML/TF risk associated with their business activity. For this purpose, the providers of payment initiation or account information services shall take into consideration all customer-related data available to them. The type of data available to depends, among others, on the specific service provided to the client with the explicit consent of the user of payment services and on the data necessary for the provision of services. In accordance with the provisions of Article 38/B(3)*f)* of Act LXXXV of 2009 on the Pursuit of the Business of Payment Services (hereinafter: Payment Services Act), providers of payment initiation services shall not request any data from the client other than the data required for the use of the payment initiation service and, in accordance with the provisions of point *g)*, it shall not use or store data or access data for any purpose other than rendering the payment initiation service expressly requested by the payer and it shall have no access to the data.

163. Monitoring: the provider of payment initiation services or account information services is expected to ensure, as part of its customer due diligence processes, that its AML/CFT system is designed to alert it to unusual or suspicious activity in relation to transactions, considering all data available to it with the express consent of the user of the payment services and necessary for the provision of its service in accordance with Article 38/B(3)*f)* and *g)* of the Payment Services Act. Providers of payment initiation or account information services shall use their own or third party typologies to detect unusual activity related to the transactions.

Customer due diligence

164. In situations of higher risk, providers of payment initiation services or account information services should apply the enhanced customer due diligence measures specified in Chapter III.

IV.11 Sector-specific guidelines for providers of currency exchange services

165. In addition to the measures specified in Chapter III hereof, providers of currency exchange services should also consider the sector-specific risk factors listed in Annex 1 along with the following measures.

166. The MNB expects that providers of currency exchange services should consider the inherent risks of currency exchange activities, which may expose them to significant ML/TF risks. Providers of currency exchange services should be aware that these risks are attributable to the simplicity, speed and often cash-based nature of the transactions. Providers of currency exchange services should also take into consideration that they may have limited knowledge of the ML/TF risk associated with the client, as clients usually execute transaction orders rather than establish a business relationship.

Measures

167. Since this business activity is primarily transaction-based, currency exchange providers should give consideration as to the type of monitoring systems and controls to be implemented to ensure that ML/TF attempts are detected even if it has only basic or no customer due diligence information on the client because no business relationship has been established. This monitoring system should be adapted to the volume of business and risk exposure.

Customer due diligence

168. The MNB expects the providers of currency exchange services to specify in their internal policies and procedures clearly when it is necessary to perform customer due diligence in respect of their ad hoc clients. The internal policies and procedures should include at least the following:

a) When the amount of a transaction or series of related transaction orders reaches or exceeds the threshold specified in point 37*b)* of Article 3 of the AML Act. A clear definition of the series of related transaction orders should be provided in the policies and procedures.

b) Cases of suspected ML/TF.

169. In all cases, the provider of currency exchange services should implement systems and controls to ensure the following:

a) series of related transaction orders (for example, to identify whether the same client visits several exchange offices belonging to the same currency exchange provider within a short period of time);

b) transaction monitoring that is appropriate and effective in the light of the risks identified during the risk assessment covering the size of the currency exchange service provider, the number of its offices, the size and volume of transactions; the type of activities performed, the service channels of the currency exchange service provider and the overall business activities of the currency exchange service provider.

Enhanced customer due diligence

170. Where the transaction order or business relationship is associated with increased risk, the provider of currency exchange services should apply enhanced customer due diligence in accordance with Chapter III, including, where appropriate, enhanced transaction monitoring (e.g. increasing the frequency or lowering the thresholds) and obtaining more information on the nature and purpose of the business activity and the source of the client's funds.

Simplified customer due diligence

171. In situations of low risk, the provider of currency exchange services may consider the use of simplified customer due diligence.

IV.12 Sector-specific guidelines related to corporate finance

172. Providers of corporate finance services should take into consideration the inherent ML/TF risks associated with these activities and bear in mind that this activity is based on close advisory relationships, especially with corporate clients and other parties, such as prospective strategic investors.

173. In addition to the provisions of Chapter III hereof, providers of corporate finance services should also consider the sector-specific risk factors listed in Annex 1 along with the measures below; in addition, the sector-specific guidelines applicable to asset management, mentioned in subtitles IV.5, IV.8 and IV.9 and addressed to investment service providers and investment fund managers may also be relevant.

Measures

174. Providers of corporate finance services collect a large volume of due diligence information due to the nature of their business. Corporate finance services providers should take into consideration this information for the purposes of preventing money laundering and terrorist financing.

Enhanced customer due diligence

175. If the business relationship or transaction is associated with increased risk, the provider of corporate finance services should apply enhanced customer due diligence measures, such as:

a) Additional verification of ownership and control structure of the client, its beneficial owners and in particular any relationships the client may have with politically exposed persons and the extent to which these relationships affect the ML/TF risk associated with the business relationship.

b) An assessment of the integrity of the directors, shareholders and other parties involved in the economic activities of the client and the corporate finance transaction to a significant degree.

c) Verification of the identity of the other owners of the company or other persons exercising control over it.

d) Identification of the source and nature of the funds or assets contributed by all parties participating in the transaction, through obtaining evidence or assurances from appropriate third parties as necessary.

e) Additional checks to determine the financial situation of the corporate client.

f) Use of non-documentary forms of evidence, such as meetings with credible persons who know the persons in question; for example, bankers, auditors or legal advisers. Providers of corporate finance services should assess whether this evidence is sufficient to demonstrate that the client has correctly presented his personal and financial circumstances. Where such non-documentary evidence is used, a register should be kept of the basis on which decisions were taken.

g) Risk-sensitive customer due diligence verifications in respect of other parties to the financial agreement to gather sufficient background knowledge to understand the nature of the transaction. This is because not only the clients of the provider of corporate finance services, but also the parties involved in the transactions, with whom the provider of corporate finance services has no direct business relationship, may pose money laundering risk to the provider of corporate finance services. Providers of corporate finance services should take into consideration that these parties may include:

i. the acquisition or merger target of the corporate client;

ii. potential or actual investors in the corporate client;

iii. companies in which the provider of corporate finance services acquires a significant shareholding (but has no wider business relationship with it);

iv. prospective clients;

v. the intermediary (which may be a supervised or non-supervised institution) acting on behalf of the securitisation special purpose vehicle in securitisation transactions defined in point 1 of Article 2

of Regulation 2017/2402/EU of the European Parliament and of the Council of 12 December 2017 laying down a general framework for securitisation and creating a specific framework for simple, transparent and standardised securitisation, and amending Directives 2009/65/EC, 2009/138/EC and 2011/61/EU and Regulations 1060/2009/EC and 648/2012/EU.

h) The provider of corporate finance services should apply enhanced and continuous monitoring. In this respect, providers of corporate finance services using automated transaction monitoring should combine automated transaction monitoring with the knowledge and expertise of the employees performing the activity. This enhanced monitoring should result in a full understanding of why the client is carrying out the transaction or activity in question. To this end, providers of corporate finance services should ensure that their employees use their knowledge of the client and what would be appropriate in the respective circumstances to detect anything that is unusual or potentially suspicious.

i) When participating in the issuance of securities, the provider of corporate finance services should ascertain that third parties involved in the sale of instruments created by securitisation instruments or securitisation transactions to investors apply appropriate customer due diligence measures of their own.

j) When assessing the ML/TF risks associated with the instruments created through securitisation or connected with securitisation transactions, the provider of corporate finance services should understand the underlying economic purpose of the scheme, including an appropriate level of due diligence performed in respect of the various parties involved in the scheme, which may include parties with whom the provider of corporate finance services has no direct business relationship.

Simplified customer due diligence

176. Due to the relationship-based nature of the corporate finance activity, the size of the transactions and the need to assess the credit and reputational risk posed by corporate finance schemes, providers of corporate finance services should use the information available to them also for the purposes of simplified customer due diligence.

177. Where the providers of corporate finance services proceed in respect of intermediaries who primarily hold accounts for the benefit of their underlying clients, the provider of corporate finance services should apply the sector-specific guidelines for investment fund managers referred to in Chapter IV.9 of this recommendation.

V. Closing provisions

178. The recommendation is a regulatory instrument, issued in accordance with Article 13(2)i) of the Act CXXXIX of 2013 on the Magyar Nemzeti Bank, with no binding force on the supervised financial organisations. The content of the recommendation issued by the MNB expresses 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.

179. 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.

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

181. The MNB expects the respective financial institutions to apply this recommendation from 1 January 2023.

182. MNB Recommendation No 7/2019 (IV. 1.) on assessing the risk of money laundering and terrorist financing associated with financial institutions and on determining related measures shall be repealed on 1 January 2023.

Annex 1 to Recommendation No 15/2022 (IX. 15.) of the Magyar Nemzeti Bank

SECTOR-SPECIFIC RISK FACTORS

The risk factors described in this Annex are not exhaustive. The MNB expects service providers to take a comprehensive view of the risk factors associated with the situation and take into consideration that the existence of certain risk factors alone does not necessarily allocate the business relationship or transaction order to a higher or lower risk category.

Risk factors related to institutions providing correspondent banking services

Risk factors

Risk factors connected to products, services and transactions

Risk increasing factors:

1. The account may be used by other banks using correspondent banking services that have a direct relationship with the bank using the respective correspondent banking services but not with the bank rendering the correspondent banking services (“nesting” or downstream clearing), which means that the correspondent bank indirectly provides services to banks other than the respondent bank.
2. The account may also be used by other institutions within the group of banks using the correspondent banking services in respect of which the bank rendering the correspondent banking services has not carried out customer due diligence.
3. The service includes the opening of a “payable through” account, which allows clients of the bank using the correspondent banking services to carry out transactions directly on behalf of the respondent bank.

Risk mitigating factors:

4. The connection is limited to the SWIFT connection Risk Management Application (RMA), which is designed to manage communication between credit institutions and financial service providers. In the SWIFT RMA relation, correspondent banks have no payment account relationship.
5. Banks act directly rather than processing transactions on behalf of their clients, for example in the case of currency exchange between two banks, where the transaction is directly concluded by the banks and does not involve a payment to a third party. In these cases, the transaction is concluded in the name of the bank using the correspondent banking service.
6. The transaction relates to the sale, purchase or pledging of securities on regulated markets, for example where the bank acts – usually through a local participant – as a custodian with direct access to an EU or non-EU securities settlement system or uses such custodian.

Customer risk factors

Risk increasing factors:

7. The policies of the bank using the correspondent banking services for the prevention of ML/TF and its systems and controls applied for the implementation of such policies do not comply with the standards specified in the AML Act and the MNB Regulation.

8. The bank using the correspondent banking service is not subject to AML/CFT supervision.

9. Recently an administrative procedure has been conducted at the bank using the correspondent banking services, at the parent company of that or at an institution rendering correspondent banking services and belonging to the same group as the bank using the service due to inadequate ML/TF policies and procedures and/or breaching the ML/TF obligations.

10. The bank using the correspondent banking services has significant business relations with sectors associated with a higher level of ML/TF risk; for example, the bank using the correspondent banking services pursues money transfer activities or conducts business with foreigners or in a currency other than its home currency on behalf of certain money transfer providers or currency exchange providers.

11. The management or owners of the bank using the correspondent banking services include politically exposed persons, especially when the politically exposed person is likely to exercise significant influence on the bank using the correspondent banking services, or if the reputation, integrity or suitability of the politically exposed person as a member of the management or as a person filling a key position raise concerns, or if the politically exposed person is from a country of higher ML/TF risk. Institutions providing correspondent banking services should pay particular attention to countries with systemic or widespread corruption.

12. The history of the business relationship with the bank using the correspondent banking services may give rise to concerns, for example because the volume of transactions is not consistent with the volume expected by the correspondent bank based on its knowledge of the nature and size of the bank using the correspondent banking services.

The bank using the correspondent banking services fails to provide the bank rendering the correspondent banking services with the information requested by the correspondent bank for the purposes of customer due diligence and enhanced customer due diligence, and the information prescribed by Regulation 2015/847/EU of the European Parliament and of the Council of 20 May 2015 on information accompanying transfers of funds and repealing Regulation 1781/2006/EC. In this respect, the correspondent bank shall act in accordance with the provisions of MNB Recommendation 1/2020 (III. 4.) on the Procedures related to the payment service providers' handling of money transfers with incomplete data.

Risk mitigating factors:

13. The AML/CFT controls of the bank using the correspondent banking service are at least as strict as the requirements of the AML Act.

14. The bank using the correspondent banking service belongs to the same group as the bank providing the correspondent banking service, or has its registered office not in a country of higher ML/TF risk and complies with group-wide anti-money laundering standards that are at least as strict as the requirements of the AML Act.

Country risk or geographical risk factors

Risk increasing factors:

15. The registered office of the bank using the correspondent banking services is located in a country of higher ML/TF risk. Institutions providing correspondent banking services should pay special attention to countries that are considered to be of higher ML/TF risk, with high levels of corruption and/or other predicate crimes connected to money laundering; have inadequate legal and judicial systems to prosecute these crimes; have significant levels of terrorist financing or terrorist activities; or lack AML/CFT supervision.

16. The bank using correspondent banking services has significant business relationship with clients located in a country of higher ML/TF risk.

17. The registered office of the parent bank of the bank using the correspondent banking services has its registered office or incorporated in a country of higher ML/TF risk.

Risk mitigating factors:

18. The bank using the correspondent banking services is located in a third country the AML/CFT requirements of which are at least as strict as those of the AML Act and it complies with these requirements. However, correspondent banks should bear in mind that the foregoing does not exempt them from the application of the measures specified in Article 24/A of the AML Act.

19. The bank using the correspondent banking service is located in an EEA country.

Risk factors related to institutions providing retail banking services

Risk factors

Risk factors connected to products, services and transactions

Risk increasing factors:

20. The product attributes give preference to anonymity.

21. The product permits payments from unidentified third parties not related to the product even if such payments are not typical, for example in the case of mortgage loans and credits.

22. The product prescribes no limit on turnover, cross-border transactions or similar product features.

23. New products and application of new business practices –including new distribution mechanisms – and new or developing technologies for both new and already existing products, when those are not yet known.

24. Lending secured by value of assets (including mortgages) in another country, particularly in countries where it is difficult to verify that the client disposes over the collateral legitimately or where it is difficult to verify the identity of the parties guaranteeing the loans.

25. Transaction of unusually large amount or high value.

Risk mitigating factors:

26. The product has limited functionality, for example:

a) a fixed-term savings product with a low savings threshold;

b) a product in which no profit can be realised to the benefit of a third party;

c) a product on which profit may be realised only in the long term or for a specific purpose, such

as a pension or property purchase;

i. a low-amount credit facility, including loans for the purchase of specific goods or services; or

ii. low-value goods, including leases, where the legal right and right to use the asset is transferred to the buyer either before the termination of the contractual relationship or not at all.

27. Only certain clients may apply for the product, such as pensioners, parents on behalf of their children or the underage until coming of age.

28 Transactions are carried out through an account under the name of the client held with a credit institution or financial service provider subject to requirements at least as strict as the statutory AML/CFT requirements.

29 There is no possibility of overpayment.

Customer risk factors

Risk increasing factors:

30. The nature of the client, such as: the client is a cash-intensive undertaking; the client is an undertaking representing higher ML risk, such as certain money transfer service providers and gambling service providers; the client is an undertaking representing higher risk of corruption, such as operating in mining or arms trade; the client is a non-profit organisation supporting countries of high TF risk; the client is a new undertaking without appropriate business profile or historical data.

a) Foreign client. Retail banks should take into consideration that Article 282/A of the Credit Institutions Act provides for the possibility for consumers legally established in an EEA State to open a basic bank account, but the right to open and use a basic payment account only applies if retail banks can comply with their AML/CFT obligations and it does not exempt retail banks from the obligation to identify and assess ML/TF risk, including the risk associated with a client without a place of abode in the Member State where the retail bank is established.

b) The beneficial owner of the client cannot be easily identified, for example because the ownership structure of the client is unusual, unduly complex or non-transparent, or because the client issues bearer shares.

31. Customer behaviour, such as:

a) The client is reluctant to provide customer due diligence information or appears to avoid personal contact deliberately;

b) The document proving the identity of the client is not of the standard form without any obvious reason;

c) The client's behaviour or the size of the transaction is not in line with the expectations related to the client’s own customer category or the information provided by the client when he opened the account;

d) The client's behaviour is unusual, for example the client unexpectedly and without reasonable explanation accelerates the agreed repayment schedule by making lump sum repayments or terminating the contract before maturity;

e) Deposits or withdraws high denomination banknotes without any obvious reason;

f) Increases his activity after a period of inactivity; or engages in transactions for which there is no apparent economic justification.

Risk mitigating factor:

32. The client is a long-standing customer with no previous transactions that gave rise to suspicion or concern and the product or service requested is consistent with the client's risk profile.

Country risk or geographical risk factors

Risk increasing factors:

33. The client's funds originate from personal or business relationships with countries of higher ML/TF risk.

34. The beneficiary is located in a country of higher ML/TF risk. Institutions providing retail banking services should pay special attention to countries known to provide financing or support for terrorist acts or to have terrorist groups operating in their territory, and to countries subject to financial sanctions, embargoes or measures related to terrorism, terrorist financing or proliferation of weapons of mass destruction.

Risk mitigating factor:

The AML/CFT systems of the countries involved in the transaction are at least as strict as the AML Act, and the countries have low levels of predicate crime.

Risk factors connected to distribution channels

Risk increasing factors:

35. Business relations established remotely without appropriate safeguards such as electronic signatures or electronic certificates issued in accordance with Regulation 910/2014/EU of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC (hereinafter: Regulation 910/2014/EU) and verifications related to identity frauds.

36. Acceptance of customer due diligence measures carried out by another service provider, if the bank has no long-standing relationship with the other service provider.

37. New, yet untested sales channels.

Risk mitigating factor:

38. The product is only available to clients who satisfy the eligibility criteria defined by the national authorities; for example beneficiaries of state allowances or savings products for children registered in a Member State.

Risk factors applicable to electronic money institutions

Risk factors

Product-related risk factors

Electronic money institutions should asses ML/TF risks connected to the following factors: thresholds; the funding method; and usefulness and marketability.

Risk increasing factors:

39. Thresholds: the product facilitates large or unlimited payments, top-ups or redemptions, including cash withdrawals; large payments, top-ups or redemptions, including cash withdrawals; storing large or unlimited amounts of funds on the electronic money product/account.

40. Funding method: the product can be funded anonymously, for example by cash, anonymous electronic money or electronic money products falling within Article 24/C of the AML Act; it can be funded by payments from unidentified third parties; it can be funded by other electronic money products.

41. Usefulness and marketability: the product facilitates person-to-person transfers; the product is accepted as a means of payment by many merchants or points of sale; the product is specifically designed to be accepted as a means of payment by merchants dealing in goods and services involving high risk of financial crime, such as online gambling; the product can be used for cross-border transactions or in different countries; the product is designed to be used by persons other than the client, for example certain co-branded card products (low value gift cards are exceptions); the product facilitates large cash withdrawals.

Risk mitigating factors:

42. Thresholds: the product: sets low payment thresholds for payments, top-ups or redemptions, including cash withdrawals (however, the electronic money institution is reminded that a low threshold alone may not be sufficient to reduce ML/TF risk); limits the number of payments, top-ups or redemptions, including cash withdrawals, that can be executed in a specific period; limits the amount of funds that can be held in an electronic money product/account at any time.

43. Funding: it is prescribed for the product that the funds for purchase or top-up are drawn from an account held with a credit institution or financial service provider in an EEA country, which is solely or jointly owned by the client.

44. Usefulness and marketability: the product prohibits or severely restricts cash withdrawals; the product can only be used inland; the product is accepted by a limited number of merchants or points of sale that are well known to the electronic money institution; the product is specifically designed for limited acceptance by merchants of goods and services involving high risk of financial crime; the product is accepted for payment for a limited number of low-risk services or products.

Customer risk factors

Risk increasing factors:

45. The customer buys several electronic money products from the same issuer, frequently tops up the product or makes several cash withdrawals within a short period of time without any economic justification; where distributors (or agents acting as distributors) are also obliged service providers, this also applies to electronic money products from different issuers bought from the same distributor.

46. The client's transactions are always immediately below the threshold.

47. The product seems to be used by several persons whose identity is not known to the issuer (for example, the product is used from several IP addresses at the same time).

48. The client’s identification data, such as address, IP address, or connected bank accounts, often change.

49 The product is used for purposes other than its intended purpose, for example, it is used overseas while it was meant to be shopping centre gift card.

Risk mitigating factor:

50. The product is only available to certain categories of clients – for example, people receiving social allowances or employees of a company that issues it as fringe benefits.

Risk factors connected to sales channels

Risk increasing factors:

51. Online and remote sales without appropriate safeguards, such as electronic signatures and electronic identification documents complying with the criteria specified in Regulation 910/2014/EU and measures against identity theft.

52. Sales through intermediaries that are not obliged service providers under the AML/CFT or the national legislation, where the electronic money institution: relies on the intermediary to comply with certain AML/CFT obligations of the electronic money institution; and it failed to ascertain that the intermediary has AML/CFT systems and controls in place.

53. Segmentation of services, i.e. the provision of electronic money services by multiple, operationally independent providers without proper supervision and coordination.

54. Before concluding a distribution agreement with a merchant, the electronic money institution should understand the merchant's business activity and purpose to ensure that the goods and services provided are legitimate and to assess the ML/TF risk associated with the merchant's business. In the case of online trading, the electronic money institution should also take measures to understand the type of customers the merchant attracts and provide the expected frequency and volume of transactions in order to detect suspicious or unusual transactions.

Country risk or geographical risk factors

Risk increasing factors:

55. The beneficiary is located in a country of higher ML/TF risk or the product is funded from resources in such country. Electronic money institutions should pay special attention to countries known to provide financing or support for terrorist acts or to have terrorist groups operating in their territory, and to countries subject to financial sanctions, embargoes or measures related to terrorism, terrorist financing or proliferation of weapons of mass destruction.

Risk factors related to institutions providing money transfer services

Risk factors

Risk factors connected to products, services and transactions

Risk increasing factors:

56. The product facilitates transactions for large or unlimited amount.

57. The product or service may be used globally.

58. The transaction is either cash-based or financed by anonymous electronic money, including electronic money falling within Article 24/C of the AML Act.

59. One or several payers in different countries make transfers to a single local beneficiary.

Risk mitigating factor:

60. The funds used for the transfer are received from an account held under the payer's name with a credit institution or financial service provider in an EEA country.

Customer risk factors

Risk increasing factors:

61. The client's business activity: the client owns or operates an undertaking that handles large amounts of cash, or the client's business has a complex ownership structure.

62. The client's activities may entail ML/TF risks, because it is publicly known to sympathise with extremism or known to be associated with an organised criminal group.

63. Customer behaviour: the client's needs could be satisfied better elsewhere, for example because the provider of the money transfer service operates at a location other than the location of the client or of its undertaking. The client obviously acts on behalf of someone else, for example, outsiders watch the client or appear further off the place of concluding the deal, or the client is reading instructions from a note. The client's behaviour lacks any obvious economic sense, for example, the customer accepts without question a poor exchange rate or high fees, initiates a transaction in a currency that is not legal tender or not in common use in the client's and/or the beneficiary's country of residence, or withdraws or deposits large amounts of currency in small or large denominations. The client's transactions are always just below the applicable thresholds, including the customer due diligence threshold for transaction orders specified in Article 6(1)*b)* of the AML Act. The institution providing the money transfer service should take into consideration that the threshold in Article 5(2) Regulation 2015/847/EU of the European Parliament and of the Council of 20 May 2015 on information accompanying transfers of funds and repealing Regulation 1781/2006/EC applies only to transactions funded from sources other than cash or from anonymous electronic money. The client uses a service in an unusual way, such as sending or receiving money to/from himself, or transferring the funds immediately after receiving it. The client apparently knows little about the beneficiary or is reluctant to provide information on it. Several clients of the money transfer service provider transfer funds to the same beneficiary, or several clients appear to have the same identification data, such as address or telephone number. The incoming transaction is not accompanied by the prescribed information on the payer or beneficiary. The amount sent or received is not line with the client's income (if known).

64. The increase in the volume or number of transactions cannot be explained by the usual pattern, such as wage transfers or holidays linked to cultural customs.

65. The client provides conflicting biographical data or identifying documents with incorrect information.

Risk mitigating factors:

66. The client is a long-standing customer of the money transfer service provider whose past behaviour has not given rise to suspicion and there are no indications that the ML/TF risk may have increased.

67. The amount transferred is small; however, the money transfer service provider should to take into consideration that small amounts alone do not reduce ML/TF risk.

Risk factors connected to sales channels

Risk increasing factors:

68. There are no restrictions on the means of financing, for example in the case of payments made from cash or electronic money products falling within the exemption provided by Article 24/C of the AML Act., bank transfers or cheques.

69. The sales channel used provides a certain degree of anonymity.

70. The service is provided entirely online, without any adequate safeguards.

71. The money transfer service is provided through payment intermediaries that: represent more than one payer; have an unusual turnover compared to other providers of money transfer services at similar locations, such as unusually high or low transaction volumes, unusually large cash transactions, or high transaction volumes just below the threshold, or conduct business outside normal business hours; conduct a high proportion of business with payers or beneficiaries from countries of higher ML/TF risk; appear to be uncertain or inconsistent in the application of AML/CFT group-wide policies; or are not from the financial sector and conduct other business activity as their core business.

72. Money transfer services are provided through an extensive network of payment intermediaries located in different countries.

73. Money transfer services are provided through an overly complex payment chain, for example through a large number of intermediaries located in different countries or through (formal and informal) settlement systems that cannot be tracked.

Risk mitigating factors:

74. Payment intermediaries are also supervised financial service providers.

75. The service can only be funded by a transfer from an account in the name of the client held with a credit institution or financial service provider in an EEA country or from an account verifiably controlled by the client.

Country risk or geographical risk factors

Risk increasing factors:

76. The payer or the beneficiary is located in a country of higher ML/TF risk or the transaction is executed from an IP address in a country of higher ML/TF risk. Providers of money transfer services should pay special attention to countries known to provide funding or support for terrorist activities, or where terrorist groups operate, or where the country is threatened with financial sanctions, embargoes or measures for terrorism, terrorist financing or proliferation.

77. The payer or the beneficiary is located in a country of higher ML/TF risk.

78. The payer is resident in a country with no or a less developed formal banking sector, which means that informal money transfer services such as “hawala” can be used at the point of payment.

79. The service partner of the provider of the money transfer services is located in a third country of higher ML/TF risk.

80. The payer or beneficiary is located in a high-risk third country with strategic deficiencies.

Risk factors related to institutions providing asset management services

Risk factors

Risk factors connected to products, services and transactions

Risk increasing factors:

81. Clients laying claim to significant amounts of cash or other physical assets such as precious metals.

82. Outstandingly high-value transactions.

83. Financial agreements involving countries of higher ML/TF risk (institutions providing asset management services should pay special attention to countries with a culture of banking secrecy or

which do not comply with international rules on tax transparency).

84. Collaterals (including mortgage loans) located in the territory of other countries, especially in countries where it is difficult to ascertain the legal basis of the collateral or where the identity of the parties guaranteeing the loan is difficult to verify.

85. Complex business structures such as fiduciary asset management and the use of private investment vehicles, especially where the identity of the ultimate beneficial owner is unclear.

86. Cross-border business activity, especially if it involves more than one financial service provider.

87. Cross-border agreements under which assets are deposited with or managed by another credit institution or financial service provider within the same group or by another credit institution or financial service provider outside the group, especially when the other credit institution or financial service provider is located in a country of higher ML/TF risk. Institutions providing asset management services should pay special attention to countries with higher levels of predicate crime, inadequate AML/CFT systems or lax tax transparency rules.

Customer risk factors

Risk increasing factors:

88. By type of client and beneficial owner:

a) Clients with income and/or assets from high-risk sectors such as the military, mining, construction and gambling sectors or private military contractors;

b) Clients who have been credibly identified as having committed an infringement;

c) Clients who expect an unusually high level of confidentiality and discretion;

d) Clients whose spending and transaction patterns make it difficult to identify “normal” or expected behavioural patterns;

e) Very wealthy and influential clients, including well-known individuals, non-resident clients and politically exposed persons. Where the client or beneficial owner is a politically exposed person, the institution providing the asset management service shall always apply enhanced customer due diligence measures pursuant to Article 16(1)*d)* of the AML Act;

f) The client requests assistance from the institution providing asset management services – without a clear business or economic justification – in obtaining a third party product or service.

Country risk or geographical risk factors

Risk increasing factors:

89. The business activity takes place in countries with a culture of banking secrecy or that do not comply with international rules on tax transparency;

90. The client lives in a country of higher ML/TF risk or his funds come from activities pursued in such country.

Risk factors related to institutions providing trade finance services

Risk factors

91. Credit institutions involved in trade finance transactions often have access only to partial information about the transaction and on the parties to it. Commercial documents can be diverse and credit institutions may not have specialised knowledge of the different types of commercial documents they receive. This may complicate the identification and assessment of ML/TF risks.

92. However, credit institutions should use sound judgement and professional assessment to decide

to what extent the information and documents in their possession may give rise to ML/TF concerns or suspicions.

93. Credit institutions should assess the following risk factors to the extent possible:

Transaction risk factors

Risk increasing factors:

94. The transaction amount is unusually large in the light of the client's former trading activities.

a) The transaction is highly structured, fragmented or complex, involving multiple parties, without any apparent legitimate reason.

b) Without reasonable explanation, copies of documents are used in situations where the use of original documents would be expected.

c) There are significant differences between documents, for example between the description of goods in the most important documents (i.e. invoices and bill of lading) and the goods actually transported, if known.

d) The type, volume and value of the goods are not in accordance with the bank's knowledge of the buyer's business.

e) The goods being the subject of the transaction represent higher risk of money laundering, for example in the case of goods the price of which may fluctuate significantly, making it difficult to detect false prices.

f) The goods being the subject of the transaction are subject to an export licence.

g) The commercial documents do not comply with the applicable laws or standards. Unit prices seem to be unusual in the light of the bank's information of prices and trade.

h) The transaction is unusual in other respects, for example, letters of credit are often amended without clear explanation or goods are transported through another country without an obvious commercial reason.

Risk mitigating factors:

95. Independent inspectors checked the quality and volume of the goods.

96. Transactions involve partners known for a long time, with a proven track record of transactions with each other and formerly they were subjected to due diligence.

Customer risk factors

Risk increasing factors:

97. The transaction and/or the parties involved in it are not consistent with the bank's knowledge of the customer's previous activities or business (for example, the goods or volumes transported are not consistent with the information on the business pursued by the importer or exporter).

98. There are signs implying that the buyer and seller collaborate, for example: the buyer and seller are controlled by the same person; the undertakings involved in the transaction have the same address, only the address of the registered authorised agent is provided, or there are other inconsistencies in the address; the buyer is willing to accept or ignore discrepancies in documents or insists on it.

99. The client is unable or unwilling to provide relevant documentation to support the transaction.

100. The buyer uses agents or third parties.

Risk mitigating factors:

101. The client is an existing customer whose business activity is well known to the bank and the transaction is consistent with that business activity.

102. The client is listed on a stock exchange that imposes similar disclosure requirements as the EU disclosure requirements.

Country risk or geographical risk factors

Risk increasing factors:

103. Currency exchange controls are in place in the country involved in the transaction (including the country of the goods' origin, the country of the goods' destination, the country of transit or the country of residence of either party to the transaction). This increases the risk that the real purpose of the transaction is to export currency breaching the local laws.
104. The country involved in the transaction has a higher level of predicate crime (such as crimes related to drug trafficking, smuggling or counterfeiting) or there are free trade zones.

Risk mitigating factors:

105. Trade takes place within the territory of the EU/EEA.
106. The AML/CFT systems of the countries involved in the transaction are at least as strict as the requirements of the AML Act, and the countries have low levels of predicate crimes.

Risk factors related to institutions providing life insurance services

Risk factors

Risk factors connected to products, services and transactions

Risk increasing factors:

107. Flexibility of payments, for example, if the product allows: payments from unidentified third parties; fee payments of large or unlimited amount, overpayments or large volume of fee payments of smaller amount; and cash payments.
108. Easy access to accumulated funds, for example, the product allows partial withdrawals or early surrender at any time, with limited costs and fees.
109. Marketability, e.g. the product: can be traded on secondary markets; can be used as collateral for a loan.
110. Anonymity; the product facilitates or enables the anonymity of the client.

Risk mitigating factors:

Connected to the product:

111. It is only paid out in the event of a predetermined event, such as death, or on a specific date, such as – in the case of life insurances taken out as a collateral for consumer and mortgage loans – which are paid out only on the death of the insured person.
112. No surrender value.
113. No investment component.
114. No top-up by third parties permitted.
115. It allows only a low amount as total investment.
116. Low premium life insurance.
117. It allows only small regular payments, no overpayments.

118. It is only available through employers – e.g. pension schemes, retirement schemes or similar schemes providing retirement benefits for employees – where contributions are paid by deduction from wages and the rules of the scheme do not allow the member to participate in the scheme.

119. Cannot be surrendered in the short or medium term, e.g. in the case of pension schemes without early surrender.

120. It cannot be used as collateral.

121. No cash deposit is permitted.

122. The use of the tax allowance is tied to conditions.

Risk factors related to clients and beneficiaries

Risk increasing factors:

123. Nature of the client, for example: legal entities the structure of which makes it difficult to identify the beneficial owner; the client or the beneficial owner of the client is a politically exposed person.

124. The beneficiary of the policy or the beneficial owner of such beneficiary is a politically exposed person; the age of the client is unusual for the requested product type (e.g. the client is very young or very old).

125. The contract is not appropriate for the client's financial situation; the client's occupation or activity is known to be highly likely to be linked to money laundering, for example because those are known to be highly cash-intensive or exposed to a high risk of corruption; the contract is signed by a "gatekeeper" such as a trust company acting on behalf of the client; the policyholder and/or the beneficiary of the policy is a company with nominee shareholders or bearer shares.

126. Customer behaviour in relation to the contract: the client often transfers the contract to another insurer; frequent and unexplained surrenders, especially when the refunds are made to different bank accounts; frequent or unexpected exercise of the free cancellation provisions or withdrawal periods, especially when the refund is made to an apparently unrelated third party; the client incurs high costs by surrendering the product; the client transfers the contract to an apparently unrelated third party; the client's request for a change and/or increase in the amount of the insured amount and/or the premium is unusual or excessive.

127. Behaviour of the client in relation to the beneficiary: the insurer is only made aware of the change of beneficiary when the claim for damages is filed; the policyholder changes the beneficiary clause and designates an apparently unrelated third party; the insurer, the policyholder, the beneficial owner, the beneficiary or the beneficial owner of the beneficiary are located in different countries.

128. Customer behaviour in relation to payments: the client uses unusual payment methods such as cash or structured monetary instruments or other payment instruments that facilitate anonymity; payments made from different bank accounts without explanation; payments made from banks established in a country other than the client's country of residence; the client makes frequent or large overpayments when not expected; payments received from unrelated third parties; convergence contribution paid to a pension close to the date of retirement.

Risk mitigating factors:

129. In the case corporate-owned life insurance, the client is:

a) A credit institution or financial service provider that is subject to AML/CFT requirements and is supervised for compliance with those requirements in accordance with the AML Act;

b) A listed public limited liability company subject to regulatory disclosure requirements (through the rules of the stock exchange, legislation or enforceable instruments) prescribing adequate transparency of the beneficial owner of the company or the majority-owned subsidiaries of such company;

c) A local government (or equivalent body) or state-owned company located in an EEA country.

Risk factors connected to sales channels

130. Risk increasing factors: Remote sales, e.g. sales over the internet, by mail or by telephone without appropriate safeguards, including among others, electronic signatures or electronic identification documents complying with Regulation 910/2014/EU of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC (eIDAS Regulation).

131. Long intermediary chains.

132. An intermediary is used in unusual circumstances (for example, from an unjustified geographical distance).

Risk mitigating factors:

133. The insurer knows the intermediaries well and ascertains that the intermediary applies customer due diligence measures proportionate to the risk associated with the relationship and complying with the requirements of the AML Act.

134. The product is only available to employees of certain companies that have concluded a contract with the insurer to provide life insurance to their employees, for example as part of a fringe benefit package.

Country risk or geographical risk factors

Risk increasing factors:

135. The insurer, the client, the beneficial owner, the beneficiary or the beneficial owner of the beneficiary is resident in or associated with a country representing higher ML/TF risk. Institutions providing life insurance services should pay special attention to countries where AML/CFT supervision is ineffective.

136. Premiums are paid from accounts held with credit institutions or financial service providers established in countries of higher ML/TF risk. Institutions providing life insurance services should pay special attention to countries where AML/CFT supervision is ineffective.

137. The intermediary is located in a country of higher ML/TF risk. Institutions providing life insurance services should pay special attention to countries where AML/CFT supervision is ineffective.

Risk mitigating factors:

138. A country is identified by credible sources – e.g. peer reviews or detailed assessment reports – as one having an efficient AML/CFT system.

139. The country is identified by credible sources as a country with low levels of corruption and other crimes.

Risk factors related to institutions engaged in investment business activities

Risk factors

Risk factors connected to products, services or transactions

Risk increasing factors:

140. The transactions are of unusually large amount;
141. Payments by third parties are permitted;
142. The product or service is used for underwriting purposes, followed shortly by redemption options, with limited intervention by the investment manager.

Customer risk factors

Risk increasing factors:

143. The customer's behaviour, e.g.
a) The investment often has no obvious economic purpose;
b) The client requests, without clear explanation, shortly after the initial investment or before the payout date, to repurchase or redeem a long-term investment, especially if this entails a financial loss or high transaction fees;
c) The client requests repeated purchases and sales of shares within a short period of time, without any obvious strategy or economic justification;
d) Lack of willingness to provide customer due diligence information on the client and the beneficial owner;
e) Frequent changes to customer due diligence information or payment details;
f) The client transfers higher amount than it is necessary for the investment and requests a refund of the excess amounts;
g) Suspicious circumstances include when the client exercises his right of withdrawal; the use of several accounts without prior notice, especially if these accounts are held in several different countries or in high-risk countries;
h) The client wishes to structure the relationship in such a way that he uses multiple parties, such as companies with nominee shareholders in different countries, especially if these countries represent higher ML/TF risk.
144. The nature of the client, for example:
a) The client is a company or a fiduciary incorporated in a country of higher ML/TF risk (institutions pursuing investment activities should pay special attention to countries that effectively do not comply with international rules on tax transparency);
b) The client is an investor that performs little or no due diligence on its own customers;
c) The client is a third party non-regulated investor;
d) The ownership and control structure of the client is non-transparent;
e) The client or beneficial owner is a politically exposed person or holds other key position that may enable him to misuse his power for personal gain;
f) The client is a non-regulated company with nominee shareholders whose shareholders are unknown.
145. The client's business activities, e.g. his funds, originate from business activities in sectors involving a high risk of financial crime.

Risk mitigating factors:

146. The client is an institutional investor whose legal status is controlled by an EEA government agency, e.g. a government-approved pension scheme.
147. The client is a general government body in an EEA country.
148. The client is a credit institution or financial service provider registered in an EEA country.

Country risk or geographical risk factors

Risk increasing factors:

149. The investor or custodian is located in a country of higher ML/TF risk.
150. The funds originate from a country of higher ML/TF risk.
151. Investment managers should know their clients thoroughly in order to help them identify the right investment portfolios. For this purpose, institutions pursuing investment activity collect information similar to that also obtained for AML/CFT purposes.

Risk factors related to institutions engaged in investment fund management activities

Risk factors

Risk factors connected to products, services or transactions

Risk increasing factors:

152. The fund was developed for a limited number of individuals or for family estate planning, such as private fund or a single investor fund.
153. It is possible to subscribe to the fund and then redeem the investment within a short period of time without the investor incurring significant administrative costs.
154. The fund's mutual fund shares can be traded without notifying the fund manager at the time of the transaction and, as a result, information about the investor is shared between several entities (as in the case of closed-end funds traded on the secondary market).

Factors increasing the risk associated with underwriting:

155. The underwriting involves accounts or third parties located in several countries, especially when these countries are of high ML/TF risk as defined in the sector-specific guidelines of this recommendation.
156. The underwriting involves third party underwriters or beneficiaries, especially when this cannot be expected.

Risk mitigating factors:

157. Payments by third parties are not permitted.
158. The fund is open to small investors only, and investments are maximised.

Customer risk factors

Risk increasing factors:

159. The customer's behaviour is unusual, e.g.:

a) The investment lacks an obvious strategy or economic purpose or the client makes investments that are not in line with the client's general financial situation, if it is known to fund manager.

b) The client requests, without clear explanation, to redeem his investment shortly after the initial investment or before the payout date, especially when this entails a financial loss or high transaction fees.

c) The client requests repeated purchases and sales of mutual fund shares in a short period of time, without any obvious strategy or economic justification.

d) The client often transfers larger amounts than it is necessary for the investment and requests a refund of the excess amounts.

e) The client uses multiple accounts without prior notice, especially if these accounts are held in several countries or in countries of higher ML/TF risk.

f) The client wishes to structure the relationship in such a way that he uses multiple parties, such as companies with nominee shareholders in different countries, especially if these countries represent higher ML/TF risk.

g) The client suddenly and without explanation changes the place of payment, e.g. he changes the country of residence.

h) The client and the beneficial owner are located in different countries and at least one of the countries represent higher ML/TF risk as defined in Chapter III of this recommendation.

i) The beneficial owner's funds were generated in a country of higher ML/TF risk, especially if the level of predicate crimes linked to money laundering and terrorist financing is higher in that country.

Risk mitigating factors:

160. The client is an institutional investor whose legal status is controlled by an EEA government agency, e.g. a government-approved pension scheme.

161. The client is an investment fund management institution in an EEA country or in a third country, where the AML/CFT requirements are at least as strict as those of the AML Act.

Risk factors connected to sales channels

Risk increasing factors:

162. Unclear or complex distribution channels that limit the fund manager's ability to understand its business relationships and monitor transactions, for example the fund uses a number of sub-distributors for marketing in third countries.

163. The distributor is located in a country of high ML/TF risk as defined in the general part of this recommendation.

Risk mitigating factors:

164. The fund only accepts a designated type of low-risk investors, such as investment fund manager institutions acting as a principal (e.g. life insurance companies) or corporate pension schemes.

165. The fund can purchased and redeemed only through an investment fund management institution, e.g. through a payment intermediary, in an EEA country or in a third country where the AML/CFT requirements are at least as strict as the requirements of the AML Act.

Country risk or geographical risk factors

Risk increasing factors:

166. Investors' funds were generated in countries of higher ML/TF risk, especially in those with higher levels of predicate crimes related to money laundering.

167. The fund invests in sectors of higher risk of corruption (such as mining or arms trade) in countries where according to credible sources the level of corruption or other predicate crimes related to money laundering and terrorist financing is high.

Risk factors related to providers of payment initiation services and account information services

Customer risk factors

Risk increasing factors:

168. In the case of a providers of payment initiation service, the client transfers funds from different payment accounts to the same beneficiary, which together amount to a large sum without a clear economic or legal justification, or the provider of payment initiation services has good reason to suspect that the client is trying to circumvent specific monitoring thresholds;

169. In the case of providers of account information services, the client transfers funds from different payment accounts to the same beneficiary, or receives funds from different payment accounts from the same payer, which together amount to a large sum without a clear economic or legal justification, or the provider of account information services has a good reason to suspect that the client is trying to circumvent specific thresholds for monitoring.

Risk factors connected to distribution channels

170. The MNB regards it as good practice if upon assessing ML/TF risks, providers of payment initiation services and account information services take into consideration the opinion of the European Supervisory Authorities on the use of innovative solutions in the customer due diligence process[10] (JC 2017 81).

Country risk or geographical risk factors

171. When assessing ML/TF risks, providers of payment initiation services and account information services should take into consideration at least the following factors that may increase the risk, especially if the client uses several accounts with different payment service providers to make payments:

a) In the case of providers of payment initiation services, the client initiates a payment to a country of higher ML/TF risk, to a third country with strategic deficiencies, to a high-risk third country or to a person known to be associated with such countries.

b) In the case of providers of account information services, the client receives funds from countries of higher ML/TF risk, from a high-risk third country with strategic deficiencies or from a person known to be associated with such countries, or the client transfers funds to a country of higher ML/TF risk, to a high-risk third country with strategic deficiencies or to a person known to be associated with

10 https://www.eba.europa.eu/sites/default/documents/files/document_library/930583/Opinion%20on%20the%20use%20of%20innovative%20solutions%20by%20credit%20and%20financial%20institutions%20%28JC-2017-81%29.pdf §

such countries, or the customer links payment accounts in more than one country in the name of several persons.

Risk mitigating factors:

172. In the case of providers of payment initiation services, the client initiates a payment transaction to an EEA member state or to third country that applies AML/CFT requirements as least as strict as those laid down in the AML Act.

173. In the case of providers of account information services, the client's payment accounts are held in an EEA country.

Risk factors related to providers of currency exchange services

Risk factors connected to products, services and transactions

Risk increasing factors:

174. The transaction is unusually large in absolute terms or compared to the economic profile of the client;

175. The transaction has no apparent economic or financial purpose.

Risk mitigating factors:

176. The exchanged amount is low. The exchange service provider should take into consideration that low amounts alone are not sufficient to eliminate ML/TF risk.

Customer risk factors

Risk increasing factors:

177. The customer’s behaviour:

a) the client's transactions are just below the applicable customer due diligence threshold, especially if these transactions occur frequently or in a short period of time;

b) the client cannot or will not provide information on the origin of the funds;

c) the client applies for the exchange of a large amount of non-convertible or infrequently used currency;

d) the customer exchanges large amounts of small denomination banknotes of a specific currency for larger denomination banknotes of another currency; or vice versa;

e) there is no apparent economic justification for the client's behaviour;

f) the customer visits several sites of the same exchange service provider on the same day (if the exchange service provider is aware of this);

g) the client asks about the identification threshold and/or refuses to answer random or routine questions;

h) the client exchanges funds in one foreign currency into another foreign currency;

i) exchange of large amounts or frequent conversions not related to the client's business activity;

j) the currency sold by the client is not in line with his country of nationality or residence;

k) the client buys currency from an unusual place compared to his own location, without a logical explanation;

l) the client purchases a currency that is not in line with the information on the client’s country of destination;

m) the client buys or sells large amounts of a currency from a country characterised by a high level

of predicate crime related to money laundering or terrorist activities.

178. The client's business activity:

the client's business activity is associated with higher risk of money laundering and terrorist financing (e.g. casinos, buying/selling precious metals and stones, waste trade).

Risk factors connected to distribution channels

Risk increasing factors:

179. The service is provided entirely online, without any adequate safeguards.

180. Services are provided through a network of intermediaries.

Country risk or geographical risk factors

Risk increasing factors:

181. The company providing the currency exchange service is located in a country of higher ML/TF risk.

Risk factors related to corporate finance

Risk factors related to clients and beneficiaries

Risk increasing factors:

182. The client's ownership structure is not transparent without an obvious commercial or legal explanation. For example, where ownership or control is exercised by other entities, such as fiduciary asset managers or securitisation special purpose vehicles defined in point 86a of Article 5(1) of Act CXX of 2001 on Capital Markets.

183. Corporate structures or transactions are complex, for example using long holding chains as shell companies or absence of transparency, and it seems to lack any reasonable business purpose.

184. There is no evidence that the client has received a mandate or approval from the competent senior executive to conclude the agreement.

185. There are few independent tools to verify the identity of the customer.

186. There is a suspicion of misconduct, such as investment fraud or insider trading.

Risk mitigating factors:

187. The client is:

a) a local government (or equivalent body) or state-owned company or an institution providing payment initiation and account information services originating from a country of low levels of corruption; or

b) a credit institution or financial service provider originating from a country with an efficient AML/CFT regime and is subject to supervision in respect of its compliance with its AML/CFT obligations.

Country risk or geographical risk factors

188. It is a risk-increasing factor when the client or beneficial owner is resident in or associated with a country representing higher ML/TF risk. The currency exchange service provider should pay particular attention to countries affected by high level of corruption.

CONTENTS