Recommendation No. 7/2019. (IV.1.) of the Magyar Nemzeti Bank

on assessing the risk of money laundering and terrorist financing associated with financial institutions and on determining related measures

I. Purpose and scope of the Recommendation

The purpose of this Recommendation is to formulate the expectations of the Magyar Nemzeti Bank (hereinafter: MNB) and thus increasing the predictability of law, facilitating the uniform application of legislation in respect of defining factors that should be considered by credit institutions and financial service providers supervised by the MNB in assessing the risk of money laundering and terrorist financing (hereinafter: ML/TF) associated with the establishment of business relationships or the execution of transaction orders. Furthermore, the Recommendation lays down how credit institutions and financial service providers supervised by the MNB should determine the level of their customer due diligence measures so that they are in proportion with the ML/TF risk identified by them.

By publishing this Recommendation, the MNB intends to provide tools with the help of which supervised credit institutions and financial service providers, while performing their activities aimed at the prevention of money laundering and terrorist financing (AML/CFT), can develop their internal risk assessment framework in line with the expectations for a risk-based approach, in a specialised manner also at the level of individual customers.

When preparing this Recommendation, the MNB took into account the guidelines published by the European financial supervisory authorities (ESAs) on 4 January 2018[1] and on 7 April 2017[2] (hereinafter jointly referred to as: ESA Guidelines). Based on the expectations formulated in the ESA Guidelines, in this Recommendation the MNB identifies the practices to be followed by supervised credit institutions and financial service providers.

The Recommendation focuses on identifying and assessing the risks of individual business relationships and occasional transactions, which should be taken into consideration by credit institutions and financial service providers supervised by the MNB in their own risk assessments related to money laundering and terrorist financing to be prepared pursuant to Section 27 of Act LIII of 2017 on the Prevention and Combating of Money Laundering and Terrorist Financing (hereinafter: AML Act), and Sections 23–29 of MNB Decree No. 45/2018. (XII. 17.) on the Rules of the Implementation of the Act on the Prevention and Combating of Money Laundering and Terrorist Financing as Applied to Credit Institutions and Financial Service Providers Supervised by the MNB and the Detailed Rules on the Minimum Requirements Applying to the Development and Operation of the Screening System Stipulated in the Act on the Implementation of Restrictive Measures Imposed by the European Union and the UN Security Council (hereinafter: MNB Decree).

The factors and measures described in the Recommendation are not exhaustive, and, where applicable, supervised credit institutions and financial service providers should also take into consideration other factors and measures.

The Recommendation is addressed to credit institutions as defined in Section 3 Subsection 16 of the AML Act and to financial service providers as defined in Section 3 Subsection 28 of the AML Act (hereinafter jointly

1 https://esas-joint-committee.europa.eu/Publications/Guidelines/Guidelines%20on%20Risk%20Factors_HU_04-01-2018.pdf

2 https://esas-joint-committee.europa.eu/Publications/Guidelines/Joint%20Guidelines%20on%20risk-based%20supervision_HU%20(ESAs%202016%2072).pdf#search=2016%2072

referred to as: service providers).

II. Definitions

For the purposes of this Recommendation:

a. ‘countries associated with higher ML/TF risk’ means countries that, based on an assessment of the risk factors set out below, present a higher ML/TF risk. This term includes, but is not limited to, ‘high-risk third countries’ identified as having strategic deficiencies in their AML/CFT regime, which pose a significant threat to the European Union’s financial system (Section 3 Subsection 31 of the AML Act).
b. ‘occasional transaction’ means a transaction that is carried out as part of an ad hoc legal relationship as defined in Section 3 Subsection 44 of the AML Act.
c. ‘pooled account’ means a bank account opened by a customer, for example a legal practitioner or notary, for holding their clients’ money. The clients’ money will be commingled on such accounts, but clients will not be able directly to instruct the bank to carry out transactions.
d. ‘risk’ means the impact and likelihood of ML/TF taking place. Risk refers to inherent risk, that is, the level of risk that exists before mitigation. It does not refer to residual risk, that is, the level of risk that remains after mitigation.
e. ‘risk factors’ means variables that, either on their own or in combination, may increase or decrease the ML/TF risk posed by an individual business relationship or occasional transaction.
f. ‘risk-based approach’ means an approach whereby supervisory authorities and service providers identify, assess and understand the ML/TF risks to which service providers are exposed and take AML/CFT measures that are proportionate to those risks.
g. ‘source of funds’ means data indicating the origin of the funds involved in a transaction, deriving from legal or illegal sources. Such legal references may include, for example, succession, compensation, entitlements – as explicitly stated – arising from civil-law contracts, income from employment, income from external service, other income, foreign exchange gains, winnings, dividends).

III. General issues of assessing and managing risks

1. The MNB requires that risk assessments consist of two distinct but related steps:

    a. identification and assessment of ML/TF risk factors; and
    b. indication of the measures determined in proportion with the degree of ML/TF risk.

2. Service providers should find out which ML/TF risks they are or would be exposed to as a result of entering into a business relationship or carrying out an occasional transaction. When identifying ML/TF risks associated with a business relationship or an occasional transaction, service providers should consider relevant risk factors including who their customer is, the countries or geographical areas they operate in, the particular products, services and transactions the customer requires and the channels the service provider uses to deliver these products, services and transactions. Service providers should take a holistic view of the risk associated with the situation and note that, unless legislation states otherwise, the presence of isolated risk factors does not necessarily move a relationship into a higher or lower risk category.

3. Service providers are expected to ensure that they have the necessary resources for implementing a risk-based strategy and their staff directly or indirectly dealing with AML/CFT tasks possesses relevant

knowledge and experience about the applicable legislative and regulatory AML/CFT framework and is appropriately trained in the interest of making reliable decisions.

4. The MNB considers it good practice that when weighting risk factors, service providers ensure the following:

   a. weighting should not be unduly influenced by just one factor;
   b. economic or profit considerations do not influence the risk rating;
   c. weighting does not lead to a situation where it is impossible for any business relationship to be classified as high risk;
   d. the risk classification of the customers is recorded in the IT systems, and the timeliness of such risk classifications is supported by automated IT solutions built in the system, depending on the risk assessment and the size of the service provider;
   e. the service provider's weighting does not override the provisions relating to situations always representing a high risk of money laundering as set out in legislation; and
   f. the service provider's risk assessment is not based exclusively on automaticity, and the service provider is able to override automatically generated risk values, where necessary. In each case the reasons for the decision relating to overriding the given values should be recorded in a retrievable manner.

5. Where a service provider uses automated IT systems to allocate overall risk scores to categorise business relationships or
   occasional transactions, and does not develop these in house but purchases them from an external provider, it should understand how the system works and how it combines risk factors to achieve an overall risk score. A service provider must always be able to satisfy itself that the scores allocated reflect the service provider's understanding of ML/TF risk and it should be able to demonstrate this to the supervisory authority.

6. When identifying the risk associated with their customers, including their customers' beneficial owners, service providers should consider the following risk factors:

   a. the customer's and the customer's beneficial owner's business or professional activity;
   b. the customer's and the customer's beneficial owner's reputation; and
   c. the customer's and the customer's beneficial owner's nature and behaviour.

7. Risk factors that may be relevant when considering the risk associated with a customer's or a customer's beneficial owner's business or professional activity include:

   a. The customer or beneficial owner has links to sectors that are commonly associated with higher corruption risk, such as construction, pharmaceuticals and healthcare, the arms trade and defence, the extractive industries or public procurement.
   b. The customer or beneficial owner has links to sectors that are associated with higher ML/TF risk, for example certain payment service providers, casinos or dealers in precious metals.
   c. The customer or beneficial owner has links to sectors that involve significant amounts of cash.
   d. Where the customer is a legal person or an unincorporated body, the purpose of their establishment or the nature of their business.
   e. The customer has domestic or foreign political connections, for example it is a politically exposed

person or its beneficial owner is a politically exposed person. The customer or beneficial owner has other relevant links to a politically exposed person, for example any of the customer's directors is a politically exposed person exercising significant control over the customer or beneficial owner. Where a customer or its beneficial owner is a politically exposed person, service providers must always apply customer due diligence measures in line with Section 19 of the AML Act.

f. The customer or beneficial owner holds another prominent position or has a prominent public-service mission that might enable them to abuse this position for private gain. For example, they are senior officials with the ability to influence the awarding of public contracts, decision-making members of high-profile sporting bodies or prominent sports federations, or individuals who are known to influence the government and other senior decision-makers.
g. The customer is a legal person subject to enforceable disclosure requirements that ensure that reliable information about the customer's beneficial owner is publicly available, for example a public company listed on stock exchanges that make such disclosure a condition for listing.
h. The customer is a credit or financial institution acting on its own account from a country with an effective AML/CFT regime and is supervised for compliance with local AML/CFT obligations, or the customer has been subject to supervisory sanctions or enforcement for failure to comply with AML/CFT obligations or other statutory requirements in recent years.
i. The customer is a public administration or enterprise from a country with low levels of corruption.
j. Whether the customer's or the beneficial owner's background is consistent with what the service provider knows about the customer's or the beneficial owner's former, current or planned business activity, their businesses' turnover or their source of funds.

8. The following risk factors are relevant when identifying the risk associated with a customer's or beneficial owner's reputation:

a. Adverse media reports or other relevant sources of information about the customer, for example allegations of criminality or terrorism against the customer
or its beneficial owner. Service providers should determine the credibility of allegations on the basis of the quality and independence of the source of the data and the persistence of reporting of these allegations, among other considerations. Service providers should note that the absence of criminal convictions alone may not be sufficient to dismiss risks.
b. The customer, beneficial owner or anyone publicly known to be closely associated with them have had their assets frozen due to administrative or criminal proceedings or allegations of terrorism or terrorist financing.
c. The service provider knows that the customer or beneficial owner has been the subject of suspicious transaction reports in the past.
d. The service provider has in-house information about the customer's or the beneficial owner's integrity, obtained, for example, in the course of a long-standing business relationship.

9. The following risk factors may be relevant when considering the risk associated with a customer's or beneficial owner's nature and behaviour; service providers should note that not all of these risk factors will be apparent at the outset; they may emerge only once a business relationship has been established:

a. The customer has legitimate reasons for being unable to provide robust evidence of its identity, perhaps because it is an asylum seeker.
b. The service provider has doubts about the veracity or accuracy of the customer's or beneficial owner's identity.

c. There are indications that the customer might seek to avoid the establishment of a business relationship, for example, the customer carries out one transaction or several one-off transactions, while the establishment of a business relationship might make more economic sense.
d. If the customer's ownership and control structure is opaque, its commercial or lawful rationale needs to be examined.
e. The customer issues bearer shares or it has nominee shareholders.
f. The customer is a legal person or an unincorporated body that operates as a trust company.
g. There are unjustified changes in the customer's ownership and control structure.
h. The customer carries out transactions that are complex, unusually or unexpectedly large, and lack an apparent economic or lawful purpose or a sound commercial rationale. There are grounds to suspect that the customer is trying to evade the threshold set out in Section 6 of the AML Act.
i. The customer requests unnecessary or unreasonable levels of secrecy. For example, the customer is reluctant to share customer due diligence information, or appears to want to disguise the true nature of its business activity.
j. The service provider requires that the customer's or beneficial owner's source of funds be easily explained, for example through their occupation, inheritance or investments. It should also take into consideration whether the customer uses the products and services it demanded when the business relationship was first established.
k. The customer's needs could be better serviced elsewhere. A sound economic and lawful rationale should be requested for the customer requesting the type of financial service sought. The service provider should note that Section 282/A(2) of Act CCXXXVII of 2013 on credit Institutions and financial enterprises (hereinafter: the Banking Act) creates a right for customers who are legally resident in an EEA state to obtain a basic payment account, but this right applies only to the extent that credit institutions can comply with their AML/CFT obligations.
l. The customer is a non-profit organisation whose activities could be abused for terrorist financing purposes.

10. When identifying the risk associated with countries and geographical areas, service providers should consider the following factors:

    a. the countries in which the customer and beneficial owner are based;
    b. the countries that are the customer's and beneficial owner's main places of business; and
    c. the countries to which the customer and beneficial owner have relevant personal links.

11. The MNB considers it good practice that service providers take into consideration that the nature and purpose of the business relationship often determines the relative importance of the risk factors of the individual countries and geographical areas:

    a. Where the funds used in the business relationship have been generated abroad, the level of predicate offences related to money laundering and the effectiveness of a country's legal system will be particularly relevant;
    b. Where funds are received from or sent to countries where groups committing terrorist offences are known to be operating, service providers should consider to what extent this could be expected to or might give rise to suspicion, based on what service providers know about the purpose and nature of the business relationship;

c. Where the customer is a credit or financial institution, service providers should pay particular attention to the adequacy of the country's AML/CFT regime and the effectiveness of AML/CFT supervision;
d. Where the customer is any other legal arrangement or a trust company,
service providers should take into account the extent to which the country in which the customer and, where applicable, the beneficial owner is established effectively complies with international tax transparency standards.

12. The MNB takes the view that service providers should consider the following risk factors when identifying the effectiveness of a country's AML/CFT regime:

a. The country's AML/CFT regime has been identified as having strategic deficiencies in in line with Section 3 Subsection 31 of the AML Act.
b. Where the service provider deals with natural or legal persons resident or established in third countries that present a high ML/TF risk, the service provider must always apply enhanced due diligence measures.
c. Information is required from more than one credible and reliable source about the quality of the country's AML/CFT controls, including information about the quality and effectiveness of regulatory enforcement and oversight. Possible sources may include the following: mutual evaluation reports by the Financial Action Task Force (FATF) or FATF-style Regional Bodies (FSRBs) (a good starting point is the executive summary and key findings and the assessment of compliance with Recommendations 10, 26 and 27, and Immediate Outcomes 3 and 4),

the FATF's list of high-risk and non-cooperative countries, International Monetary Fund (IMF) assessments and Financial Sector Assessment Programme (FSAP) reports. Service providers should note that membership of the FATF or an FSRB (e.g. MoneyVal) does not, of itself, mean that the country's AML/CFT regime is adequate and effective.

13. Service providers should note that Decree No 28/2008. (X. 10.) PM of the Ministry of Finance on third countries applying requirements equivalent to those set out in
Act CXXXVI of 2007 on the Prevention and Combating of Money Laundering and Terrorist Financing
was repealed on 26 June 2017. The MNB requires that to the extent permitted by national legislation, service providers should identify lower risk countries in line with this Recommendation and Chapter 4 of the MNB Decree. When identifying the level of terrorist financing risk associated with a country, service providers should primarily consider the following
risk factors:

a. Information from law enforcement or other credible and reliable open media sources, suggesting that a country provides funding or support for terrorist activities or that groups committing terrorist offences are known to be operating in the country or territory.
b. Whether the country is subject to financial sanctions, embargoes or measures that are related to terrorism, terrorist financing or the proliferation of weapons of mass destruction issued by the United Nations or the European Union.

14. When identifying a country's level of transparency and tax compliance, service providers should take into consideration the following risk factors:

a. Information from more than one credible and reliable source is required concerning that the country is compliant with international tax transparency and information sharing standards, and information that relevant rules are effectively implemented in practice. Examples of possible sources include, for example, the following: reports by the Global Forum on Transparency and the Exchange of Information for Tax Purposes of the Organisation for Economic Co-operation and Development (OECD), which rate countries for tax transparency and information sharing purposes; assessments of the country's commitment to automatic exchange of information based on the Common Reporting Standard; assessments of compliance with FATF Recommendations 9, 24 and 25 and Immediate Outcomes 2 and 5 by the FATF or FSRBs; and IMF assessments (e.g. IMF staff assessments of offshore financial centres).
b. Whether the country has committed to, and effectively implemented, the Common Reporting Standard on Automatic Exchange of Information, which the G20 adopted in 2014.
c. Whether the country has put in place reliable and accessible beneficial ownership registers.

15. Risk factors that service providers should consider when identifying the risk associated with the level of predicate offences related to money laundering include the following:

a. Information from credible and reliable public sources about the level of predicate offences related to money laundering– such as corruption offences, organised crime, serious budget fraud – as defined in Act C of 2012 on the Criminal Code,
for example: corruption perceptions indices, OECD country reports on the implementation of the OECD's anti-bribery convention, and the United Nations Office on Drugs and Crime World Drug Report.
b. Information from more than one credible and reliable source about the capacity of the country's investigative and judicial system to effectively investigate and prosecute such offences.

Essential risk factors associated with the transparency of a product, service or transaction include:

16. When identifying the risk associated with their products, services or transactions, service providers should consider the risk related to the following:

a. The should examine the extent to which products or services allow the customer or beneficial owner or beneficiary structures to remain anonymous, or facilitate hiding their identity. Examples of such products and services include: bearer shares, fiduciary deposits, offshore vehicles and certain trusts, and foundations that can be structured in such a way as to take advantage of anonymity and allow dealings with shell companies or companies with shareholders owning bearer shares.
b. A third party that is not part of the business relationship can give instructions, for example in the case of certain correspondent banking relationships.

17. Essential risk factors associated with the complexity of a product, service or transaction include:

a. The extent of the complexity of the transaction and whether it involves multiple parties or countries. Products or services allow payments from third parties, or overpayments are accepted even this would not normally be expected. During risk assessment it is regarded as a risk mitigating factor, if the products and services are funded by transfers from the customer's own account at another financial institution that is subject to AML/CFT standards and oversight that are

comparable to those required under the AML Act.

b. Risks associated with its new or innovative product or service, in particular where this involves the use of new technologies or payment methods.

18. Essential risk factors associated with the value or size of a product, service or transaction include:

a. The products and services are cash intensive, for example payment services and certain current accounts.

b. The products and services facilitate or encourage high-value transactions. Caps applied on transaction values or levels of premium should be examined, because the application of caps could limit the use of the product or service for ML/TF purposes.

19. When identifying the risk associated with the products or services used by the customer, the following factors should be taken into consideration:

a. If the customer is not physically present for identification purposes, it may be necessary to take steps to prevent impersonation or identity fraud. b. If the customer was identified by another entity of the same financial group, it should be examined to what extent the service provider can rely on this due diligence audit as reassurance that the customer will not expose it to excessive ML/TF risk. The service provider should satisfy itself that the group entity applied due diligence measures in line with Section 22(5) of the AML Act.

c. If customer due diligence was carried out by a third party, for example a bank that is not part of the same group,
it should be examined whether the third party is a financial institution or whether its main business activity is related to financial service provision.

20. It is recommended to record what the service provider has done to satisfy itself that:

a. the third party applies due diligence measures and keeps records according to EEA standards, and it is supervised for compliance with AML/CFT obligations in line with Section 22(3)a) of the AML Act;

b. the third party provides, immediately upon request, relevant copies of identification and verification documents, inter alia in line with Section 23(1)–(2) of the AML Act; and

c. the quality of the third party's customer due diligence measures is such that it can be relied upon.

d. If customer due diligence was carried out through a tied agent, that is, without direct contact with the service provider,
it is necessary to make sure that the agent has obtained enough information for the service provider to get to know its customer and the level of risk associated with the business relationship.

e. If independent or tied agents are used, it is necessary to find out to what extent they are involved in establishing the business relationship, and how this affects the service provider's knowledge of the customer and ongoing risk management.

f. If the service provider uses an intermediary, the following should be examined: whether the intermediary is a supervised person subject to AML obligations that are consistent with those set out in the AML Act; whether the intermediary is subject to effective AML supervision, or whether there are any indications that the intermediary's level of compliance with applicable AML legislation or regulation is inadequate, for example whether the intermediary has been sanctioned

for breaches of AML/CFT obligations; whether the intermediary is based in a country associated with higher ML/TF risk. Where a third party is based in a high-risk third country that the Commission has identified as having strategic deficiencies, the service provider must not rely on that intermediary. However, to the extent permitted by legislation, reliance may be possible provided that the intermediary is a branch or majority-owned subsidiary of another service provider established in the Union, and the service provider is confident that the intermediary fully complies with group-wide policies and procedures in line with Chapter 15 of the AML Act.

Simplified customer due diligence

21. To the extent permitted by legislation, service providers may apply simplified due diligence measures in situations where the ML/TF risk associated with a business relationship has been assessed as low. Simplified customer due diligence is not an exemption from any of the required customer due diligence measures, however, service providers may adjust the amount, timing or type of each or all of the customer due diligence measures in a way that is commensurate to the low risk they have identified.
22. Simplified customer due diligence measures service providers may apply primarily include the following:

    a. Determining the time of customer due diligence, for example where the product or transaction sought has features that limit its use for ML/TF purposes, for example by: verifying the customer's identity during the establishment of the business relationship; or verifying the customer's identity once transactions exceed a defined threshold or once a reasonable time limit has lapsed. Service providers must make sure that this does not result in a de facto exemption from customer due diligence, i.e. that the customer's identity will ultimately be verified; the threshold or time limit is set at a reasonably low level (although, with regard to terrorist financing, service providers should note that a low threshold alone may not be enough to reduce the risk); they have systems in place to detect when the threshold or time limit has been reached; and they do not defer customer due diligence or delay obtaining relevant information about the customer where applicable legislation requires that this information be obtained at the start of the relationship.
    b. Adjusting the quantity of information obtained for identification, verification or monitoring purposes, for example by: verifying the customer's identity on the basis of information obtained from one single reliable, credible and independent document or data source only; or determining the nature and purpose of the business relationship based on that the product can be used for one particular use only, for example for a company pension scheme or for a shopping centre gift card.
    c. Adjusting the quality or source of information obtained for identification, verification or monitoring purposes, for example by: accepting information obtained primarily from the customer rather than an independent source when verifying the beneficial owner's identity (note that this is not permitted in relation to the verification of the customer's identity); or where the risk associated with all aspects of the relationship is very low, relying on the source of funds to meet some of the customer due diligence requirements, for example where the funds are state benefit payments or where the funds have been transferred from an account in the customer's name with a service provider established in an EEA state.
    d. Adjusting the frequency of customer due diligence updates and reviews of the business relationship, for example carrying these out only when trigger events occur such as the customer looking to take out a new product or service or when a certain transaction threshold is reached; service providers must make sure that this does not

result in a de facto exemption from keeping customer due diligence information up-to-date.

e. adjusting the frequency and intensity of transaction monitoring, for example by monitoring transactions above a certain threshold only. Where service providers choose to do this, they must ensure that the threshold is set at a reasonable level and that they have systems in place to identify linked transactions that, together, would exceed that threshold. Service providers are expected to take into consideration the results deriving from the prescribed monitoring activity during their procedures.

23. The information a service provider obtains when applying simplified due diligence measures must enable the service provider to be reasonably satisfied before introducing such measures that its assessment that the risk associated with the relationship is low is justified. The measures must also be sufficient to give the service provider enough information about the nature of the business relationship to identify any unusual or suspicious transactions. Simplified due diligence does not exempt institutions from their obligation to report suspicious transactions to the financial information unit.

24. Section 18 of the MNB Decree contains a description of the cases when service providers can carry out simplified customer due diligence. Pursuant to the risk-based approach, however, service providers may also identify cases other than those described in the Decree, where it finds that simplified due diligence is required. In respect of such cases, however, a risk assessment effect study must be prepared, and the MNB's approval is required. The MNB grants its approval by continuously extending the group of cases included in the Decree, in order to make sure that service providers compete under equal conditions.

25. Where there are indications that the risk may not be low, for example where there are reasonable grounds to suspect money laundering or terrorist financing, or where the service provider has doubts about the veracity of the information obtained, simplified due diligence may not be applied.

Enhanced customer due diligence

26. The MNB considers it appropriate that service providers apply enhanced due diligence measures in higher risk situations to manage and mitigate those risks appropriately. Enhanced due diligence measures cannot be substituted for regular customer due diligence measures, but they should be applied in addition to regular customer due diligence measures.

27. The following specific cases – in addition to those specified in legislation – must always be treated by service providers as high risk:

    a. where the customer or the customer's beneficial owner is a politically exposed person;
    b. where a service provider enters into a correspondent banking relationship with an institution from a non-EEA state;
    c. where a service provider deals with natural persons or legal entities residing or established in high-risk third countries; and

    d. all complex and unusually large transactions, or unusual types of transactions that have no obvious economic or lawful purpose.

28. In addition to the specific cases set out in legislation, service providers should apply further enhanced due diligence measures in situations where this is commensurate to the ML/TF risk they have identified.

29. Enhanced due diligence measures to be applied by service providers include, in particular, the following:

    a. Information about the customer's or beneficial owner's identity, or the customer's ownership and control structure, to be satisfied that the risk associated with the relationship is well understood. This may include obtaining and assessing information about the customer's or beneficial owner's reputation and assessing any negative allegations against the customer or beneficial owner. For example: information about family members and close business partners; information about the customer's or beneficial owner's past and present business activities; and adverse media searches.
    b. Information about the intended nature of the business relationship to ascertain that the nature and purpose of the business relationship is legitimate and to help service providers to obtain a more complete customer risk profile. This may include obtaining information on the following: the number, size and frequency of transactions that are likely to pass through the account, to enable the service provider to spot deviations that might give rise to suspicion of money laundering (in some cases, requesting evidence may be appropriate).
    c. It must be clarified why the customer is looking for a specific product or service, in particular where use of such product or service would be more appropriate in a different country;
    d. determining the destination of funds;
    e. the nature of the customer's or beneficial owner's business, to enable the service provider to better understand the likely nature of the business relationship.

30. Increasing the quality of information obtained for customer due diligence purposes to confirm the customer's or beneficial owner's identity including by:

    a. requiring the first payment to be carried out through an account verifiably in the customer's name with a bank subject to standards that are not less robust than those set out in Chapter 4 of the MNB Decree; or
    b. establishing that the customer's funds used in the business relationship are not the proceeds of criminal activity and that the source of funds is consistent with the service provider's knowledge of the customer and the nature of the business relationship. In some cases, where the risk associated with the customer relationship is particularly high, verifying the source of funds may be the only adequate risk mitigation tool. The source of funds can be verified, inter alia, by reference to VAT and income tax returns, copies of audited accounts, pay slips, public deeds or independent media reports.

31. Increasing the frequency of reviews to be satisfied that the service provider continues to be able to manage the risk associated with the individual business relationship or conclude that the relationship no longer corresponds to the service provider's risk appetite and to help identify any transactions that require further review, including by:

    a. increasing the frequency of reviews of the business relationship to ascertain whether the customer's risk profile has changed and whether the risk remains manageable;
    b. obtaining the approval of senior management to commence or continue the business relationship to ensure that senior management are aware of the risk their service provider is exposed to and

can take an informed decision about the extent to which the service provider is equipped to manage that risk;

c. reviewing the business relationship on a more regular basis to ensure any changes to the customer's risk profile are identified and, where necessary, acted upon; or conducting more frequent or in-depth transaction monitoring to identify any unusual or unexpected transactions that might give rise to suspicion of ML/TF. This may include establishing the destination of funds or ascertaining the reason for certain transactions.

32. The MNB requires that service providers keep their assessments of the ML/TF risk associated with individual business relationships and occasional transactions as well as the underlying factors under review to ensure that their assessment of ML/TF risk remains up to date. Service providers should assess information obtained in the scope of monitoring business relationships and consider whether such information affects the risk assessment.

33. Service providers should also ensure that they have systems and controls in place to identify emerging ML/TF risks and that they can assess these risks and, where appropriate, incorporate them into their business-wide and individual risk assessments in a timely manner.

34. The systems, processes and controls that service providers should put in place to identify emerging risks include:

a. Processes to ensure that internal information is reviewed regularly to identify trends and emerging issues, in relation to both individual business relationships and the service provider's business activity.

b. Processes to ensure that the service provider regularly reviews the information sources specified in the Recommendation. This should involve, in particular, the following: regularly reviewing media reports that are relevant to the sectors or countries in which the service provider is active; regularly reviewing law enforcement alerts and reports; ensuring that the service provider becomes aware of changes to terror alerts and sanctions regimes as soon as they occur, for example by regularly reviewing terror alerts and looking for sanctions regime updates; and regularly reviewing thematic reviews and similar publications issued by supervisory authorities.

c. Processes to capture and review information on risks relating to new products.

d. Engagement with other industry representatives and supervisory authorities (e.g. round tables, conferences and training courses), and feedback on potential findings to the relevant staff.

e. Establishing a culture of information sharing and strong company ethics in respect of the service provider.

35. Examples of systems and controls – regarded as good practice by the MNB – that service providers should put in place to ensure their individual and business-wide risk assessments remain up to date may include:

a. Setting a date on which the next risk assessment update will take place, for example on 1 March every year, to ensure new or emerging risks are included in risk assessments. Where the service provider is aware that a new risk has emerged or an existing risk has increased, this should be reflected in risk assessments as soon as possible.

b. Carefully recording issues throughout the year that could have a bearing on risk assessments, such

as internal suspicious transaction reports, compliance failures and intelligence from front office staff.

c. Like the original risk assessments, any update to a risk assessment and adjustment of accompanying customer due diligence measures should be proportionate and commensurate to the ML/TF risk.

Systems and controls

36. Service providers should take the necessary measures to ensure that their risk management systems and controls, in particular those relating to the application of the right level of customer due diligence measures, are effective and proportionate.

Record keeping

37. Service providers should record and document their risk assessments of business relationships, as well as any changes made to risk assessments as part of their reviews, in order to ensure that they can demonstrate to the supervisory authorities that their risk assessments and associated risk management measures are adequate.

IV. Sector-specific guidelines

38. The MNB requires that service providers also use sector-specific guidelines, which complement the general requirements. Sector-specific guidelines should be interpreted in conjunction with the general requirements. Sector-specific risk factors to be considered are listed in the Annex to the Recommendation.

Sectoral guidelines for institutions providing correspondent banking services

39. In identifying correspondent banking relationships, primarily the provisions of Section 3 Subsection 23 of the AML Act
should be taken into consideration.

40. In a correspondent banking relationship, the correspondent provides banking services to the respondent, either in a principal-to-principal capacity or on the respondent's customers' behalf. The correspondent does not normally have a business relationship with the respondent's customers and will not normally know their identity or the nature or purpose of the underlying transaction, unless this information is included in the payment instruction. Banks should consider the risk factors
set out in Annex 1. The MNB considers it good practice that following due consideration of the risk factors,
the following measures are implemented, in particular.

Measures

41. Correspondent banks are required to carry out customer due diligence on the respondent, who is the correspondent's customer, on a risk-sensitive basis, in the scope of which the following measures must be taken:

a. Identify, and verify the identity of the respondent and its beneficial owner. As part of this,

correspondent banks should obtain sufficient information about the respondent's business and reputation to establish that the money-laundering risk associated with the respondent is not increased. In particular, correspondents should:

i. obtain information about the respondent's management and consider the relevance, for financial crime prevention purposes, of any links the respondent's management or ownership might have to politically exposed persons or other high-risk individuals; and
ii. consider, on a risk-sensitive basis, whether obtaining information about the respondent's major business, the types of customers it attracts, and the quality of its AML systems and controls (including publicly available information about any recent regulatory or criminal sanctions for AML failings) would be appropriate. Where the respondent is a branch, subsidiary or affiliate, correspondents should also consider the status, reputation and AML controls of the parent.
iii. It is recommended to establish and document the nature and purpose of the service provided, as well as the responsibilities of each institution. In the framework of this, the MNB finds it good practice to set out, in writing, the scope of the relationship, which products and services will be supplied, and how and by whom the correspondent banking facility can be used (e.g. if it can be used by other banks through their relationship with the respondent).
iv. It is recommended to monitor the business relationship, including transactions, to identify changes in the respondent's risk profile and detect unusual or suspicious behaviour, including activities that are not consistent with the purpose of the services provided or that are contrary to commitments that have been concluded between the correspondent and the respondent. Where the correspondent bank allows the respondent's customers direct access to accounts (e.g. payable-through accounts or nested accounts), it should conduct enhanced monitoring. Due to the nature of the correspondent banking relationship, post-execution monitoring is the norm.
v. It must be ensured that the customer due diligence information is up to date.

42. Practically, correspondents should also establish that the respondent does not permit its accounts to be used by a shell bank, in line with Section 18(3) of the AML Act. This may include asking the respondent for confirmation that it does not deal with shell banks, having sight of relevant passages in the respondent's policies and procedures, or considering publicly available information, such as legal notices that prohibit the servicing of shell banks.

43. Correspondents should bear in mind that customer due diligence questionnaires provided by international organisations are not normally designed specifically to help correspondents comply with their obligations under the AML Act. In order to ensure compliance with the obligations under the AML Act, correspondents should assess whether the use of these questionnaires will be sufficient, or they should take additional steps.

Correspondent banks based in non-EEA countries

44. The MNB requires that where the respondent is based in a third country, pursuant to Section 18 of the AML Act correspondents apply enhanced due diligence measures in addition to the customer due diligence measures set out in Sections 7–8

of the AML Act.

45. Correspondents must apply each of these enhanced due diligence measures to respondents based in a non-EEA country, but correspondents can adjust the extent of these measures on a risk-sensitive basis. For example, if the correspondent is satisfied that the respondent is based in a country that has an effective AML/CFT regime and is supervised effectively for compliance with AML/CFT requirements, and that there are no grounds to suspect that the respondent's AML policies and procedures are, or have recently been deemed, inadequate, then the assessment of the respondent's AML controls may not necessarily have to be carried out in full detail.

46. Correspondents should always adequately document their customer due diligence and enhanced due diligence measures and decision-making processes.

47. Section 18 of the AML Act requires correspondents to take risk-sensitive measures to:
    a. Gather sufficient information about a respondent institution to understand fully the nature of the respondent's business

       in order to establish the extent to which the respondent's business exposes the correspondent to higher money-laundering risk. This should include taking steps to understand and risk-assess the nature of the respondent's customer base and the type of activities that the respondent will transact through the correspondent account.
    b. Determine from publicly available information the reputation of the institution and the quality of supervision. This means that the correspondent should assess the extent to which the correspondent can take comfort from the fact that the respondent is adequately supervised for compliance with its AML obligations. A number of publicly available resources (for example FATF or FSRB assessments), which contain sections on effective supervision
       may help correspondents establish this.
    c. Assess the respondent institution's AML/CFT controls. This implies that the correspondent should carry out a qualitative assessment of the respondent's AML/CFT control framework, not just obtain a copy of the respondent's AML policies and procedures. This assessment should be documented appropriately. In line with the risk-based approach, where the risk is especially high and in particular where the volume of correspondent banking transactions is substantive, the correspondent should consider on-site visits and/or sample testing to be satisfied that the respondent's AML policies and procedures are implemented effectively.
    d. Obtain approval from senior management, as defined in Section 3 Subsection 35 of the AML Act, before establishing new correspondent relationships. The approving senior manager should not be the officer sponsoring the relationship, and the higher the risk associated with the relationship, the more senior the approving senior manager should be. Correspondents should keep senior management informed of high-risk correspondent banking relationships and the steps the correspondent takes to manage that risk effectively.
    e. Document the responsibilities of each institution. This may be part of the correspondent's standard terms and conditions, but correspondents should set out in writing how and by whom the correspondent banking facility can be used (e.g. if it can be used by other banks through their relationship with the respondent), and
       what the respondent's AML/CFT responsibilities are.
       Where the risk associated with the relationship is high, it may be appropriate for the correspondent to satisfy itself that the respondent complies with its responsibilities under this

agreement, for example through ex post transaction monitoring.

f. With respect to payable-through accounts and nested accounts, be satisfied that the respondent credit or financial institution has verified the identity of and performed ongoing due diligence on the customer having direct access to accounts of the correspondent, and that it is able to provide relevant customer due diligence data to the correspondent institution upon request. Correspondents should seek to obtain confirmation from the respondent that the relevant data can be provided upon request.

Correspondent banks based in EEA countries

48. Where the respondent is based in an EEA country, the correspondent is required to apply risk-sensitive customer due diligence measures.
49. Where the risk associated with a respondent based in an EEA Member State is increased, correspondents should apply enhanced due diligence measures in line with Section 18 of the AML Act.

Sectoral guidelines for institutions providing retail banking services

50. Due to the nature of the products and services offered, the relative ease of access and the often large volume of transactions and business relationships, retail banking is vulnerable to terrorist financing and to all stages of the money laundering process. At the same time, the volume of business relationships and transactions associated with retail banking can make identifying ML/TF risk associated with individual relationships and spotting suspicious transactions particularly challenging.
51. Banks should consider the following risk factors and measures set out in Annex 1. The MNB finds it goods practice that after considering the risk factors the following measures be implemented.

Measures

52. Where banks use automated systems to identify ML/TF risk associated with individual business relationships or occasional transactions and to identify suspicious transactions, they should ensure that these systems are fit for purpose in line with the criteria set out in legislation and in this Recommendation. The use of automated IT systems should never be considered a substitute for staff vigilance.

Enhanced customer due diligence

53. Where the risk associated with a business relationship or occasional transaction is increased, banks should apply enhanced due diligence measures. These may include:

    a. Verifying the customer's and the beneficial owner's identity on the basis of more than one reliable and independent source.
    b. Identifying and verifying the identity of other shareholders who are not the customer's beneficial owners or any natural persons who have authority to operate an account or give instructions concerning the transfer of funds or the transfer of securities.
    c. Obtaining more information about the customer and the nature and purpose of the business relationship to build a more complete customer profile, for example by carrying out open source or adverse media searches or commissioning a third party intelligence report. Examples of the type of information banks may seek include: the nature of the customer's business or employment; the source of the customer's funds that are involved in the customer's business relationships, to be

reasonably satisfied that these are legitimate; the purpose of the transaction, including, where appropriate, the destination of the customer's funds; other associations the customer might have with other countries (headquarters, operating facilities, branches, etc.) and the individuals who may influence its operations;

or where the customer is based in another country, why it seeks retail banking services in a different country.

d. Increasing the frequency of transaction monitoring.
e. Reviewing and, where necessary, updating information and documentation held more frequently. Where the risk associated with the relationship is particularly high, banks should review the business relationship annually.

Simplified customer due diligence

54. In low-risk situations, and to the extent permitted by national legislation, banks may apply simplified due diligence measures approved by the supervisory authority, which may include the following:

    a. for customers that are subject to a statutory licensing and regulatory regime, obtaining evidence to demonstrate this, for example through a search of the regulator's public register;
    b. verifying the customer's and, where applicable, the beneficial owner's identity after the establishment of the business relationship in accordance with Section 13(2) of the AML Act;
    c. assuming that a payment drawn on an account in the sole or joint name of the customer at a regulated credit or financial institution in an EEA country satisfies the requirements stipulated in Section 7 and Sections 8–9 of the AML Act;
    d. updating customer due diligence information only in case of specific trigger events, such as the customer requesting a new or higher risk product, or changes in the customer's behaviour or transaction profile that suggest that the risk associated with the relationship is no longer low.

Pooled accounts

55. Where a bank's customer opens a 'pooled account' in order to administer funds that belong to its own clients, the bank should apply full customer due diligence measures, including treating the customer's clients as the beneficial owners of funds held in the pooled account and verifying their identities. Where there are indications that the risk associated with the business relationship is high, banks are recommended to apply enhanced due diligence measures.

56. However, to the extent permitted by legislation, where the risk associated with the business relationship is low, and subject to the conditions set out below, banks may apply simplified due diligence measures provided that

    a. The customer is a service provider that is subject to AML/CFT obligations in an EEA state or a third country with an AML/CFT regime that is not less robust than that required by the AML Act, and is supervised effectively for compliance with these requirements.
    b. The customer is not a service provider, but in another EEA state it is an obliged service provider that is subject to AML/CFT obligations and is supervised effectively for compliance with these

requirements.

c. The ML/TF risk associated with the business relationship is low, based on the bank's assessment of its customer's business, the types of clients the customer's business serves and the countries the customer's business is exposed to, among other considerations;
d. the bank is satisfied that the customer applies robust and risk-sensitive customer due diligence measures to its own clients and its clients' beneficial owners (it may be appropriate for the bank to take risk-sensitive measures to assess the adequacy of its customer's CDD policies and procedures, for example by liaising directly with the customer); and
e. the bank has taken risk-sensitive steps to be satisfied that the customer will provide customer due diligence information and documents on its underlying clients that are the beneficial owners of funds held in the pooled account immediately upon request, for example by including relevant provisions in a contract with the customer or by sample-testing the customer's ability to provide customer due diligence information upon request.

57. Where the conditions for the application of simplified due diligence to pooled accounts are met, following approval by the supervisory authority, simplified due diligence measures may consist of the bank:

a. identifying and verifying the identity of the customer, including the customer's beneficial owners (but not the customer's underlying clients);
b. assessing the purpose and intended nature of the business relationship; and
c. conducting ongoing monitoring of the business relationship.

Sectoral guidelines for institutions providing electronic money issuing services

58. Electronic money means electronically – including magnetically – stored monetary value as represented by a claim on the issuer, which is issued on receipt of funds for the purpose of making payment transactions, and which is accepted by a natural or legal person other than the electronic money issuer.

59. Electronic money can only be issued by credit institutions and financial service providers authorised to do so, by the European Central Bank, national central banks and Member States' local and regional authorities. Prepaid cards and e-wallets are dominant in the field of electronic money. With regard to the fact that the use of electronic money can be suitable for the anonymous movement of funds, e-money institutions need to apply a risk-sensitive approach and consider what customer due diligence procedures they should carry out in connection with the use of the services and products provided by them.

Measures

60. Regardless of the level of risk, service providers should ensure that they obtain sufficient information about their customers or the types of customers their product will target, to be able to carry out meaningful ongoing monitoring of the business relationship. The monitoring systems
service providers should put in place include:

a. transaction monitoring systems that detect anomalies or suspicious patterns of behaviour,

including the unexpected use of the product in a way for which it was not designed; the service provider should be able to disable the product either manually or through on-chip controls until it has been able to satisfy itself that there are no grounds for suspicion;

b. systems that identify discrepancies between submitted and detected information, for example, between submitted country of origin information and the electronically detected IP address;
c. systems that compare data submitted with data held by the bank on other business relationships and that can identify patterns such as the same funding instrument or the same contact details;
d. systems that identify whether the product is used with merchants dealing in goods and services that are associated with a high risk of financial crime.

Enhanced customer due diligence

61. Enhanced customer due diligence measures to be applied in high-risk situations:

a. obtaining additional customer information during identification, for example about the source of funds;
b. applying additional verification measures from a wider variety of reliable and independent sources (e.g. checking against online databases) in order to verify the customer's or beneficial owner's identity;
c. obtaining additional information about the intended nature of the business relationship, for example by asking customers about their business or the countries to which they intend to transfer electronic money;
d. obtaining information about the merchant/payee, in particular where the e-money issuer has grounds to suspect that its products are being used to purchase illicit or age-restricted goods;
e. verifying identity to prevent abuse;
f. applying strengthened procedure to the customer relationship and the individual transactions;
g. establishing the source and/or the destination of funds.

Simplified customer due diligence

62. Apart from the cases of exemption specified in Section 15(3)–(4) of the AML Act, the MNB does not support the application of simplified due diligence measures.

Sectoral guidelines for institutions providing money remittance services

63. Money remittance is a simple payment service generally based on cash provided by the remitting party to the service provider, by sending, via a communication channel, the relevant amount to the addressee or to another payment service provider acting on behalf of the addressee. As many payment service providers primarily carry out transaction-based activities, it is recommended that service providers consider what type of monitoring systems and controls they should use to detect ML/TF attempts, even if they hold only basic customer due diligence information or no such information at all about the customer, as no business relationship has been established.

Measures

64. Service providers should put in place:

a. systems to identify linked transactions;
b. systems to identify whether transactions from different customers are destined for the same payee;
c. systems to permit as far as possible the establishment of the source of funds and the destination of funds;
d. systems that allow the full traceability of both transactions and the number of operators included in the payment chain; and
e. systems to ensure that throughout the payment chain only those duly authorised to provide money remittance services can intervene.

Use of agents

65. The MNB requires that money remitters using agents to provide payment services know who their agents are. As part of this, money remitters should establish and maintain appropriate and risk-sensitive policies and procedures to counter the risk that their agents may engage in, or be used for ML/TF, including by:

    a. Identifying the person who owns or controls the agent where the agent is a legal person, to be satisfied that the ML/TF risk to which the money remitter is exposed as a result of its use of the agent is not increased.
    b. Obtaining evidence, in line with the requirements of Section 55(3) of Act CCXXXV of 2013 on certain payment service providers that the directors and other persons responsible for the management of the agent are fit for executing their tasks, including by considering their honesty, integrity and reputation. Any enquiry the money remitter makes should be proportionate to the nature, complexity and scale of the ML/TF risk inherent in the payment services provided by the agent and could be based on the money remitter's customer due diligence procedures.
    c. Taking reasonable measures to satisfy themselves that the agent's AML/CFT internal controls are appropriate and remain appropriate throughout the agency relationship, for example by monitoring a sample of the agent's transactions or reviewing the agent's controls on site. Where an agent's internal AML/CFT controls differ from the money remitter's, for example because the agent represents more than one principal or because the agent is itself a service provider under AML/CFT legislation, the money remitter should practically assess and manage the risk that these differences might affect its own or the agent's AML/CFT compliance.
    d. It is recommended to provide AML/CFT training to agents to ensure that agents have an adequate understanding of relevant ML/TF risks and the quality of the AML/CFT controls the money remitter expects.

Sectoral guidelines for institutions providing wealth management services

Measures

66. The staff member managing a wealth management firm's relationship with a customer (the relationship manager) plays a key role in assessing risk. The relationship manager's close contact with the customer will facilitate the collection of information that allows a fuller picture of the purpose and nature of the customer's business to be formed (e.g. an understanding of the customer's source of funds, why complex or unusual arrangements may nonetheless be genuine and legitimate, or why extra security may be required). This close contact may, however, also lead to conflicts of interest if the relationship

manager becomes too close to the customer, to the detriment of the service provider's efforts to manage the risk of financial crime. Consequently, independent oversight of risk assessment may also be required, provided by, for example, the compliance department and senior management.

Enhanced customer due diligence

67. The following enhanced due diligence measures may be appropriate in high-risk situations. Obtaining and verifying more information about customers than in standard risk situations, and reviewing and updating this information both on a regular basis and when prompted by material changes to the customer's profile. Service providers should perform reviews on a risk-sensitive basis, reviewing higher risk customers at least annually, or more frequently, if necessary. These procedures may include those for recording any visits to customers' premises, whether at their home or business, including any changes to customer profile or other information that may affect risk assessment that these visits prompt.
    a. Establishing the source of funds; where the risk is particularly high or where the service provider has doubts about the legitimate origin of the funds, verifying the source of funds may be the adequate risk mitigation tool. The source of funds can be verified, by reference to, inter alia: an original or certified copy of the most recent pay slip; written confirmation of annual salary signed by the employer; an original or certified copy of contract of sale of investments or a company; written confirmation of sale signed by a solicitor; an original or certified copy of a will or grant of probate; written confirmation of inheritance signed by a solicitor, trustee or executor; an internet search of a company registry to confirm the sale of a company.
    b. Establishing the destination of funds.
    c. Performing greater levels of scrutiny and due diligence on business relationships than would be typical in mainstream financial service provision, such as in retail banking or investment management.
    d. Carrying out an independent internal review and, where appropriate, seeking senior management approval of new clients and existing clients on a risk-sensitive basis.
    e. Monitoring transactions on an ongoing basis, including reviewing each transaction as it occurs, to detect unusual or suspicious activity. This may include measures to determine whether any of the following are out of line with the business risk profile: transfers (of cash, investments or other assets); wire transfers; significant changes in activity; transactions involving countries associated with higher ML/TF risk.

68. Monitoring measures may include the use of thresholds, and a review process by which unusual behaviours can be promptly reviewed by relationship management staff or (at certain thresholds) the compliance functions or senior management.

    a. Monitoring public reports or other sources of intelligence to identify information that relates to customers or to their known associates, businesses to which they are connected, potential corporate acquisition targets or third party beneficiaries to whom the customer makes payments.
    b. Ensuring that cash or other physical stores of value (e.g. travellers' cheques) are handled only at bank counters, and never by relationship managers, as far as possible.
    c. Ensuring that the service provider is satisfied that a customer's use of complex business structures – such as trusts and private investment vehicles – is for legitimate and genuine purposes, and that the identity of the ultimate beneficial owner is understood.

Simplified customer due diligence

69. The MNB does not recommend simplified due diligence in the case of wealth management.

Sectoral guidelines for trade finance providers

70. Trade finance means managing payment to facilitate the movement of goods (and the provision of services) either domestically or across borders. When goods are shipped internationally, the importer faces the risk that the goods will not arrive, while the exporter may be concerned that payment will not be forthcoming. To lessen these dangers, many trade finance instruments therefore place banks in the middle of the transaction.

71. Trade finance can take many different forms. These include:

    a. 'Open account' transactions: these are transactions where the buyer makes a payment once it has received the goods. These are the most common means of financing trade, but the underlying trade-related nature of the transaction will often not be known to the banks executing the fund transfer. Banks should practically refer to the sector-specific prescriptions included in this Recommendation to manage the risk associated with such transactions.
    b. Documentary letters of credit (LCs): an LC is a financial instrument issued by a bank that guarantees payment to a named beneficiary (typically an exporter) upon presentation of certain 'complying' documents specified in the credit terms (e.g. evidence that goods have been dispatched).
    c. Documentary bills for collection (BCs): a BC refers to a process by which payment or an accepted draft is collected by a 'collecting' bank from an importer of goods for onward payment to the exporter. The collecting bank gives the relevant trade documentation (which will have been received from the exporter, normally through their bank) to the importer in return.

72. Other trade finance products such as forfaiting or structured financing, or wider activities such as project finance, are outside the scope of this Recommendation. Banks offering these products should refer to the general guidance included in the sector-specific prescriptions of this Recommendation. Trade finance products can be abused for money-laundering or terrorist financing purposes. For example, the buyer and seller may collude to misrepresent the price, type, quality or quantity of goods in order to transfer funds or value between countries.

73. The International Chamber of Commerce (ICC) has developed standards that govern the use of LCs and BCs, but these do not cover matters related to financial crime. The MNB recommends that the affected service providers take into consideration that the use of these standards does not mean that banks do not need to comply with their AML/CFT obligations. Service providers in this sector should consider the risk factors and measures set out in Annex 1 to this Recommendation. The MNB finds it goods practice that after considering the risk factors the following measures be implemented.

74. Banks party to trade finance transactions often have access only to partial information about the transaction and the parties to it. Trade documentation can be diverse and banks may not have expert knowledge of the different types of trade documentation they receive. This can make the identification and assessment of ML/TF risk challenging. Banks should, nevertheless, use common sense and professional judgement to assess the extent to which the information and documentation they have could give rise to concern or suspicion of ML/TF.

Measures

75. The MNB requires that banks carry out customer due diligence on the instructing party. In practice, most banks accept instructions only from existing customers and the wider business relationship that the bank has with the customer may assist its due diligence efforts.

76. Where a bank provides trade finance services to a customer, it should take steps, as part of its customer due diligence process, to understand its customer's business. The bank can obtain information for example about the following: the countries with which the customer trades, which trading routes are used, which goods are traded, who the customer does business with (buyers, suppliers, etc.), whether the customer uses agents or third parties, and, if so, where these are located. This should help banks understand who the customer is and detect unusual or suspicious transactions.
77. Where a bank is a correspondent, it must apply due diligence measures to the respondent. In addition to taking into consideration the risk factors specified in Annex 1 to this Recommendation, correspondent banks should follow the guidelines included in this Recommendation.

Enhanced customer due diligence

78. In higher risk situations, banks must apply enhanced due diligence. As part of this, banks should consider whether performing more thorough due diligence checks on the transaction itself and on other parties to the transaction (including non-customers) would be appropriate.

79. Checks on other parties to the transaction may include:

    a. Taking steps to better understand the ownership or background of other parties to the transaction, in particular where they are based in a country associated with higher ML/TF risk or where they handle high-risk goods. This may include checks of company registries and third party intelligence sources, and open source internet searches.
    b. Obtaining more information on the financial situation of the parties involved.
    c. Checks on transactions may include, inter alia, the following: using third party or open source data sources – for example the International Maritime Bureau (for warning notices, bills of lading, shipping and pricing checks) –, or using shipping lines' free container tracking service to verify the information provided and to check that the purpose of the transaction is legitimate;
    d. using professional judgement to consider whether the pricing of goods makes commercial sense, in particular in relation to traded commodities for which reliable and up-to-date pricing information can be obtained;
    e. checking that the weights and volumes of goods being shipped are consistent with the shipping method.

80. Since LCs and BCs are largely paper-based and accompanied by trade-related documents (e.g. invoices, bills of lading and manifests), automated transaction monitoring may not be feasible. The processing bank should assess these documents for consistency with the terms of the trade transaction and require staff to use professional expertise and judgement to consider whether any unusual features warrant the application of enhanced due diligence measures or give rise to suspicion of ML/TF.

Simplified customer due diligence

81. The checks banks routinely carry out to detect fraud and ensure that transactions conform to the standards set by the International Chamber of Commerce mean that, in practice, they may not apply simplified due diligence measures even in lower risk situations.

Sectoral guidelines for institutions providing life insurance services

Life insurance products are designed to financially protect the policy holder against the risk of an uncertain future event, such as death, illness or outliving savings in retirement (longevity risk). Protection is achieved by an insurer who pools the financial risks that several different policy holders are faced with. Life insurance products can also be bought as investment products or for pension purposes, the savings element and risk coverage can be purchased under the same contract (as a so-called unit-linked product or as a traditional life insurance product). Due to the nature of insurance risks, term insurance policies are also very important, in the case of which the contract does not include a section on savings/investment. In the case of the latter product type, the risk of money laundering is extremely low. There are single premium and regular premium life insurance policies, and in the case of contracts also containing a savings element customers typically have the opportunity to pay an incidental premium for the contract on top of the undertaken premium payment.

Life insurance products are provided through different distribution channels to customers who may be natural or legal persons or unincorporated bodies. The beneficiary of the contract may be the policy holder or a nominated or designated third party; the beneficiary may also change during the term, and the original beneficiary may never benefit from the life insurance.

Most life insurance products are designed for the long term, and they typically
pay out on a verifiable event specified in the contract, such as death or retirement. This means that many life insurance products are not sufficiently flexible to be the first vehicle of choice for money launderers. However, as with other financial service products, there is a risk – although lower than average – that the funds used to purchase life insurance may be the proceeds of crime.

82. Besides the risk factors and measures set out in the sector-specific prescriptions of this Recommendation, service providers should consider the following. In this context the sectoral guidelines for wealth management and for investment firms may also be relevant. Where intermediaries are used, the risk factors associated with the delivery channel will be relevant. Intermediaries may also find these guidelines useful.

Measures

83. Section 13(3)–(4) of the AML Act provides that, for life insurance business, service providers must apply customer due diligence measures not only to the customer and beneficial owner but also to the beneficiaries as soon as they are identified or designated. This means that service providers must:

    a. Obtain the name of the beneficiary where either a natural or legal person or an unincorporated body is identified as the beneficiary; or

    b. Obtain sufficient information to be satisfied that the identities of the beneficiaries can be established at the time of payout where the beneficiaries are a class of persons or designated by certain characteristics. For example, where the beneficiary is ‘my future grandchildren’, the insurer may obtain information about the policy holder’s children.

c. Verify whether payments of the insured sum were actually made to the beneficiaries specified in the insurance contract already scrutinised. From the aspect of preventing money laundering, the recipients of payments of insured sums must be regarded as beneficiaries in each case, regardless of whether they have been specified as such in the insurance contract.

d. Service providers must verify the beneficiaries' identities at the latest at the time of payout. Where the service provider knows that the life insurance has been assigned to a third party who will receive the value of the policy, it must identify the beneficial owner at the time of the assignment.

Enhanced customer due diligence

The following enhanced due diligence measures may be appropriate in high-risk situations:

84. Where the customer makes use of the free cancellation/cooling-off period, the premium should be refunded to the customer's bank account from which the funds were paid. Service providers should ensure that they have verified the customer's identity before making a refund, in particular where the premium is large or the circumstances appear otherwise unusual. Service providers should also consider whether the cancellation gives rise to suspicion of money laundering, and whether submitting a suspicious activity report would be appropriate.

85. Additional steps may be taken to strengthen the service provider's knowledge about the customer, the beneficial owner, the beneficiary or the beneficiary's beneficial owner, third party payers and payees. Such measures may include the following:

a. non-application of the prescription in Section 13(2), which provides for an exemption from upfront customer due diligence;

b. verifying the identity of other relevant parties, including third party payers and payees, before the beginning of the business relationship;

c. obtaining additional information to establish the intended nature of the business relationship; obtaining additional information on the customer and updating more regularly the identification data of the customer and beneficial owner;

d. if the payer is different from the customer, establishing the reason why;

e. verifying identities on the basis of more than one reliable and independent source;

f. establishing the customer's source of funds, for example by obtaining data on employment and salary, inheritance or divorce settlements;

g. where possible, identifying the beneficiary at the beginning of the business relationship, rather than waiting until they are identified or designated at a later point, bearing in mind that the beneficiary can change over the term of the policy;

h. identifying and verifying the identity of the beneficiary's beneficial owner;

i. in line with Sections 19 and 20 of the AML Act, taking measures to determine whether the customer is a politically exposed person, or whether the beneficiary or the beneficiary's beneficial owner is a politically exposed person at the time of the assignment, in whole or in part, of the policy or, at the latest, at the time of payout;

j. requiring the first payment to be carried out through an account in the customer's name with a

bank subject to customer due diligence standards that are not less robust than those required under the AML Act.

86. Section 19(2)–(4) and (5) requires that, where the risk associated with a business relationship with politically exposed persons is high, service providers must not only apply customer due diligence measures in line with Sections 7–10 of the AML Act, but also inform senior management before the payout of the policy so that senior management can take an informed view of the ML/TF risk associated with the situation and decide on the most appropriate measures to mitigate that risk; in addition, service providers must conduct enhanced due diligence on the entire business relationship.

87. More frequent and more in-depth monitoring of transactions may be required (including, where necessary, obtaining information on the source of funds).

Simplified customer due diligence

88. The following customer due diligence measures may be taken in low-risk situations (to the extent permitted by legislation):
    a. Service providers may be able to assume that the verification of the identity of the customer is fulfilled on the basis of a payment drawn on an account that the service provider is satisfied is in the sole or joint name of the customer with an EEA-regulated credit institution.
    b. Service providers may be able to assume that the verification of the identity of the beneficiary of the insurance policy is fulfilled on the basis of a payment made to an account in the beneficiary's name at a regulated EEA credit institution.

Sectoral guidelines for investment firms

89. Investment management is the management of an investor's assets to achieve specific investment goals. It includes both discretionary investment management, where investment managers take investment decisions on their customers' behalf, and advisory investment management, where investment managers advise their customers on which investments to make but do not execute transactions on their customers' behalf.

90. Investment managers usually have a limited number of private or institutional customers, many of which are wealthy, for example high-net-worth individuals, trusts, companies, government agencies and other investment vehicles. The customers' funds are often handled by a local custodian, rather than the investment manager. The ML/TF risk associated with investment management is therefore driven primarily by the risk associated with the type of customers investment managers serve.

91. The MNB recommends that besides the risk factors and measures set out in Annex 1 to this Recommendation, service providers in this sector should also consider the following. In low-risk situations investment managers can use simplified due diligence measures specified in the sector-specific prescriptions of this Recommendation, to the extent allowed by legislation.

Measures

92. Investment managers are expected to develop a good understanding of their customers to help them

identify suitable investment portfolios. For this, service providers gather information similar to that obtained for AML/CFT purposes.

93. In higher risk situations service providers are recommended to follow the enhanced due diligence measures set out in the general part (Chapter III) of this Recommendation. In addition, where the risk associated with a business relationship is high, service providers should:

    a. identify and, where necessary, verify the identity of the underlying investors of the customers where the customer is an unregulated third-party investor;
    b. understand the reason for any payment or transfer to or from an unverified third party.

94. In low-risk situations investment managers can use simplified due diligence measures specified in the general part (Chapter III) of this Recommendation, to the extent allowed by legislation.

95. The MNB requires that supervised institutions identify the underlying investors of their customers, and, where necessary, verify their identity, where the customer is an unregulated third-party investor.

96. Supervised institutions need to understand the reason for any payment or transfer to or from an unverified third party.

Sectoral guidelines for providers of investment funds

97. The requirements included in this chapter are applicable to the fund manager's activity involving the distribution of units of investment funds, as set out in Section 3 Subsection 28 l) of the AML Act.

98. The type and number of parties involved in the process of distributing units of investment funds depends, among other things, on the nature of the fund and may affect how much the fund manager distributing the units of investment funds knows about its customers and investors. The fund manager will retain responsibility for compliance with AML/CFT obligations, with regard to the fact that the scope of the AML Act does not cover investment funds themselves or fund managers not involved in the distribution of units of investment funds, but it only covers the distribution activity of the fund manager distributing units of investment funds.

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

    a. Retail funds are often distributed on a non-face-to-face basis; access to such funds is often easy and relatively quick to achieve, and holdings in such funds can be transferred between different parties.
    b. Alternative investment funds, such as hedge funds, real estate and private equity funds, tend to have a smaller number of investors, which can be private individuals as well as institutional investors (pension funds, funds of funds). Funds that are designed for a limited number of high-net-worth individuals, or for family offices, can have an inherently higher risk of abuse for ML/TF purposes than retail funds, since investors are more likely to be in a position to exercise control over the fund's assets.
    c. Notwithstanding the often medium- to long-term nature of the investment, which can contribute to limiting the attractiveness of these products for money laundering purposes, they may still

appeal to money launderers on the basis of their ability to generate growth and income.

100. Other parties involved in the distribution of units of investment funds, for example intermediaries, are also recommended to comply with their own customer due diligence obligations and should refer to relevant chapters of this Recommendation, as appropriate.

101. In high-risk situations, fund managers distributing units of investment funds should apply, among others, the following enhanced due diligence measures:

a. obtaining additional customer information, for example about the customer's reputation and background, before the establishment of the business relationship;
b. taking additional steps to further verify the documents, data or information obtained;
c. obtaining information on the source of funds of the customer and its beneficial owner;
d. requiring that redemption payment be made through the initial account used for investment or an account in the sole or joint name of the customer;
e. increasing the frequency and intensity of transaction monitoring;
f. requiring that the first payment be made through a payment account held in the sole or joint name of the customer with an EEA-regulated credit or financial institution, or a regulated credit or financial institution in a third country that has AML/CFT requirements that are not less robust than those set out in the AML Act;
g. obtaining approval from senior management at the time of concluding the transaction, when a customer uses a product or service for the first time;
h. applying a strengthened procedure in respect of the customer relationship and the individual transactions.

102. In lower risk situations, to the extent permitted by legislation, and provided that the funds are verifiably being transferred to or from a payment account held in the customer's sole or joint name with an EEA-regulated credit or financial institution, an example of the simplified due diligence measures that may be applied by the fund manager distributing units of investment funds is using the source of funds to meet some of the customer due diligence requirements.

103. In situations concerning the customer, where the financial intermediary is the customer of the fund manager distributing units of investment funds, the fund manager distributing units of investment funds should apply risk-sensitive customer due diligence measures in respect of the financial intermediary. The fund manager distributing units of investment funds should also take risk-sensitive measures to identify, and verify the identity of, the investors underlying the financial intermediary, as these investors are beneficial owners of the funds invested through the intermediary. To the extent permitted by legislation, in low-risk situations,
fund managers distributing units of investment funds may apply simplified due diligence measures similar to those described in the section of this Recommendation describing simplified due diligence measures applicable in the case of pooled accounts, subject to the following conditions:

a. The financial intermediary is subject to AML/CFT obligations in an EEA country or in a third country that has AML/CFT requirements that are not less robust than those set out in the AML Act.
b. The financial intermediary is effectively supervised for compliance with these requirements.
c. The fund manager distributing units of investment funds has taken risk-sensitive steps to be satisfied that the ML/TF risk associated with the business relationship is low, based on, inter alia,

the assessment of the financial intermediary's business, the types of customers the intermediary's business serves and the countries the intermediary's business is exposed to.

d. The fund manager distributing units of investment funds has taken risk-sensitive steps to be satisfied that the intermediary applies robust and risk-sensitive customer due diligence measures to its own customers and its customers' beneficial owners. As part of this, the fund manager distributing units of investment funds should take risk-sensitive measures to assess the adequacy of the intermediary's customer due diligence policies and procedures, for example by referring to publicly available information about the intermediary's compliance record or by liaising directly with the intermediary.
e. The fund manager distributing units of investment funds has taken risk-sensitive steps to be satisfied that the intermediary will provide customer due diligence information and documents on the underlying investors immediately upon request, for example by including relevant provisions in a contract with the intermediary or by sample-testing the intermediary's ability to provide customer due diligence information upon request.

104. Where the risk is increased, in particular where the fund is designated for a limited number of investors, enhanced due diligence measures should apply, which may include those set out below.

The fund manager distributing units of investment funds should apply risk-sensitive customer due diligence measures to the ultimate investor. To meet its customer due diligence obligations,

the fund manager distributing units of investment funds may rely upon the intermediary in line with, and subject to, the conditions set out in Sections 22–23 of the AML Act.

b. To the extent permitted by legislation, in low-risk situations, fund managers distributing units of investment funds may apply simplified due diligence measures. Provided that the conditions listed above are met, simplified due diligence measures may consist of the fund manager receiving identification data as specified in Section 23(1) of the AML Act, which the fund manager should practically obtain from the intermediary within a reasonable timeframe. The fund manager should set that timeframe in line with the risk-based approach.

V. Final provisions

105. This Recommendation is a regulatory instrument issued within the meaning of Section 13(2)i) of the Act on the Magyar Nemzeti Bank, with no binding force for the supervised financial organisations. The contents of the Recommendation issued by the MNB reflect statutory requirements, the principles and methods proposed for application based on the procedural practices of the MNB, and the prevailing market standards and practices.

106. In line with the general European supervisory practice, compliance with the Recommendation among the financial organisations subject to the MNB's supervision shall be monitored and assessed in the course of the MNB's control and monitoring activities.

107. The MNB advises the relevant organisations that they are permitted to incorporate the contents of this Recommendation into their internal regulations. In such cases, the financial organisation is entitled to state that the provisions set out in its regulations comply with the relevant MNB recommendation. If the financial organisation wishes to incorporate only certain parts of the Recommendation into its internal regulations, it should refrain from referring to the Recommendation or limit such references to

the parts transposed from the Recommendation.

108. The MNB expects financial organisations to apply this Recommendation as from 1 May 2019.

Dr. György Matolcsy, sgd.,
Governor of the Magyar Nemzeti Bank

Annex to Recommendation No. 7/2019. (IV.1.) of the Magyar Nemzeti Bank

SECTOR-SPECIFIC RISK FACTORS

The list of risk factors described in this Annex is not exhaustive. The MNB requires service providers to adopt a comprehensive approach to the risk factors associated with the various situations, and take into consideration that the presence of isolated risk factors does not necessarily move a business relationship or an occasional transaction into a higher or lower risk category.

Risk factors associated with institutions providing correspondent banking services

Risks factors

Product, service and transaction risk factors

The following factors may contribute to increasing risk:

1. The account can be used by other respondent banks that have a direct relationship with the respondent but not with the correspondent ('nesting' or downstream clearing), which means that the correspondent is indirectly providing services to other banks other than the respondent.
2. The account can be used by other entities within the respondent's group that have not themselves been subject to the correspondent's due diligence.
3. The service includes the opening of a payable-through account, which allows the respondent's customers to carry out transactions directly on the account of the respondent.

The following factors may contribute to reducing risk:

4. The relationship is limited to a SWIFT (RMA) relationship, which is designed to manage communications between financial institutions. In a SWIFT RMA relationship correspondent banks do not have a payment account relationship.
5. Banks are acting in a principal-to-principal capacity, rather than processing transactions on behalf of their customers, for example in the case of foreign exchange services between two banks where the business is transacted on a principal- to-principal basis between the banks and where the settlement of a transaction does not involve payment to a third party. In those cases, the transaction is for the own account of the respondent bank.
6. The transaction relates to the selling, buying or pledging of securities on regulated markets, for example when the bank acts as or uses a custodian with direct access – usually through a local participant – to an EU or non-EU securities settlement system.

Customer risk factors

The following factors may contribute to increasing risk:

7. The respondent's AML/CFT policies and the systems and controls the respondent has in place to implement them fall short of the standards required by Act LIII of 2017 on the Prevention and Combating of Money Laundering and Terrorist Financing (AML Act).

8. The respondent is not subject to AML/CFT supervision.
9. The respondent, its parent or a supervised institution belonging to the same group as the respondent has recently been the subject of regulatory enforcement for inadequate AML/CFT policies and procedures and/or breaches of AML/CFT obligations.
10. The respondent conducts significant business with sectors that are associated with higher levels of ML/TF risk; for example, the respondent conducts remittance business or business on behalf of certain money remitters or exchange houses, with non-residents or in a currency other than that of the country in which it is based.
11. The respondent's management or ownership includes politically exposed persons, in particular where a politically exposed person can exert meaningful influence over the respondent, where the politically exposed person's reputation, integrity or suitability as a member of the management board or key function holder gives rise to concern, or where the politically exposed person is from a country associated with higher ML/TF risk. Supervised institutions should pay particular attention to those countries where corruption is perceived to be systemic or widespread.
12. The history of the business relationship with the respondent gives rise to concern, for example because the amount of transactions are not in line with what the correspondent would expect based on its knowledge of the nature and size of the respondent.

The following factors may contribute to reducing risk:

13. The respondent's AML/CFT controls are not less robust than those required by the AML Act.
14. The respondent is part of the same group as the correspondent, or it is not based in a country associated with higher ML/TF risk, and it complies with group AML standards that are not less strict than those required by the AML Act.

Country or geographical risk factors

The following factors may contribute to increasing risk:

15. The respondent is based in a country associated with higher ML/TF risk. Supervised institutions should pay particular attention to countries where there is a high level of corruption and/or other predicate offences related to money laundering; where there is no adequate legal and judicial system to effectively prosecute those offences; or where there is no AML/CFT supervision.
16. The respondent conducts significant business with customers based in a country associated with higher ML/TF risk.
17. The respondent's parent is established or is incorporated in a country associated with higher ML/TF risk.

The following factors may contribute to reducing risk:

18. The respondent is based in an EEA Member State.

The respondent is based in a third country that has AML/CFT requirements not less robust than those set out in the AML Act, and effectively implements those requirements. At the same time, correspondent banks should note that this does not exempt them from applying the measures set out in Section 18 of the AML Act.

Risk factors associated with institutions providing retail banking services

Risks factors

Product, service and transaction risk factors

The following factors may contribute to increasing risk:

19. The product's features favour anonymity;
20. The product allows payments from third parties that are neither associated with the product nor identified upfront, where such payments would not be expected, for example for mortgages or loans;
21. The product places no restrictions on turnover, cross-border transactions or similar product features; new products and new business practices, including new delivery mechanisms, and the use of new or developing technologies for both new and existing products, where these are not yet known;
22. Lending (including mortgages) secured against the value of assets in other countries, particularly countries where it is difficult to ascertain whether the customer has legitimate title to the collateral, or where the identities of parties guaranteeing the loan are hard to verify;
23. Transactions of unusually high volume or large value.

The following factors may contribute to reducing risk:

24. The product has limited functionality, for example in the case of:
    a. a fixed term savings product with low savings thresholds;
    b. a product where the benefits cannot be realised for the benefit of a third party;
    c. a product where the benefits are only realisable in the long term or for a specific purpose, such as pension or a property purchase;
    d. a low-value loan facility, including loans conditional on the purchase of specific consumer goods or services;

    e. or a low-value product, including a lease, where the legal and beneficial title to the asset is not transferred to the customer until the contractual relationship is terminated, or is never passed at all.
    f. The product can only be held by certain categories of customers, for example pensioners, parents on behalf of their children, or minors until they reach the age of majority.
    g. Transactions are carried out through an account in the customer's name at a credit or financial institution that is subject to AML/CFT requirements that are not less robust than those set out in legislation.
    h. There is no overpayment facility.

Customer risk factors

The following factors may contribute to increasing risk:

25. The nature of the customer, for example: the customer is a cash-intensive undertaking; the customer is an undertaking associated with higher levels of money laundering risk, for example certain money remitters and gambling businesses; the customer is an undertaking associated with a higher corruption risk, for example operating in the extractive industries or the arms trade; the customer is a non-profit

organisation that supports countries associated with an increased TF risk; the customer is a new undertaking without an adequate business profile or track record.

a. The customer is a non-resident. Banks should note that Section 282/A of the Banking Act creates a right for consumers who are legally resident in an EEA state to open a basic bank account, although the right to open and use a basic payment account applies only to the extent that banks can comply with their AML/CFT obligations, and it does not exempt banks from their obligation to identify and assess ML/TF risk, including the risk associated with the customer not being a resident of the Member State in which the bank is based.

b. The customer's beneficial owner cannot be identified easily, for example because the customer's ownership structure is unusual, unduly complex or opaque, or because the customer issues bearer shares.

26. The customer's behaviour, for example:

a. The customer is reluctant to provide customer due diligence information or appears to avoid face-to-face contact deliberately;

b. The customer's evidence of identity is in a non-standard form for no apparent reason;

c. The customer's behaviour or the transaction volume is not in line with that expected from the customer category to which it belongs,
or with the information the customer provided at account opening.

d. The customer's behaviour is unusual, for example the customer unexpectedly and without reasonable explanation accelerates an agreed repayment schedule, by means of lump sum repayments or early termination of the contract;

e. Deposits or demands payout of high-value bank notes without apparent reason;

f. Increases activity after a period of dormancy; or makes transactions that appear to have no economic rationale.

The following factor may contribute to reducing risk:

27. The customer is a long-standing client whose previous transactions have not given rise to suspicion or concern, and the product or service sought is in line with the customer's risk profile.

Country or geographical risk factors

The following factors may contribute to increasing risk:

28. The customer's funds originate from personal or business links to countries associated with higher ML/TF risk.
29. The payee is located in a country associated with higher ML/TF risk. Supervised institutions should pay particular attention to countries known to provide funding or support for terrorist activities or where groups committing terrorist offences are known to be operating, and countries subject to financial sanctions, embargoes or measures that are related to terrorism, terrorist financing or the proliferation of weapons of mass destruction.

The following factor may contribute to reducing risk:

30. Countries associated with the transaction have an AML/CFT regime that is not less robust than that required under the AML Act, and are associated with low levels of predicate offences.

Distribution channel risk factors

The following factors may contribute to increasing risk:

31. Non-face-to-face business relationships, where no adequate safeguards – for example electronic signatures, electronic identification certificates issued in accordance with 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, or anti-impersonation fraud checks – are in place;
32. Reliance on consumer due diligence measures implemented by another service provider, where the bank does not have a long-standing relationship with such other service provider;
33. New delivery channels that have not been tested yet.

The following factor may contribute to reducing risk:

34. The product is available only to customers who meet specific eligibility criteria set out by national authorities; this is the situation for example in the case of state benefit recipients or specific savings products for children registered in a particular Member State.

Risk factors associated with institutions providing electronic money issuing services

Risks factors

Product risk factors

35. E-money issuers should consider the ML/TF risk related to the following: thresholds; the funding method; and utility and negotiability.

The following factors may contribute to increasing risk:

36. Thresholds: the product allows the following: high-value or unlimited-value payments, loading or redemption, including cash withdrawal; high-value payments, loading or redemption, including cash withdrawal; high or unlimited amount of funds to be stored on the e-money product/account.
37. Funding method: the product can be loaded anonymously, for example with cash, anonymous e-money or e-money products covered by Section 15(3)–(4) of the AML Act; the product can be funded with payments from unidentified third parties; the product can be funded with other e-money products.
38. Utility and negotiability: the product allows person-to-person transfers; the product is accepted as a means of payment by a large number of merchants or points of sale; the product is designed specifically to be accepted as a means of payment by merchants dealing in goods and services associated with a high risk of financial crime, for example online gambling; the product can be used in cross-border transactions or in different countries; the product is designed to be used by persons other than the customer, for example certain partner card products (but not low-value gift cards); the product allows high-value cash withdrawals.

The following factors may contribute to reducing risk:

39. Thresholds: the product sets low-value limits on payments, loading or redemption, including cash withdrawal (although supervised institutions should note that a low threshold alone may not be enough to reduce TF risk); the product limits the number of payments, loading or redemption, including cash withdrawal in a given period; the product limits the amount of funds that can be stored on the e-money product/account at any one time.
40. Funding: the product requires that the funds for purchase or reloading are verifiably drawn from an account held in the customer's sole or joint name at an EEA credit or financial institution;
41. Utility and negotiability: the product does not allow or strictly limits cash withdrawal; the product can be used only domestically; the product is accepted by a limited number of merchants or points of sale, with whose business the e-money issuer is familiar; the product is designed specifically to restrict its use by merchants dealing in goods and services that are associated with a high risk of financial crime; the product is accepted as a means of payment for limited types of low-risk services or products.

Customer risk factors

Risk factors associated with institutions providing money transfer services

The following factors may contribute to increasing risk:

42. The customer purchases several e-money products from the same issuer, frequently reloads the product or makes several cash withdrawals in a short period of time and without an economic rationale; where distributors (or agents acting as distributors) are obliged service providers themselves, this also applies to e-money products of different issuers purchased from the same distributor.
43. The customer's transactions are always just below the value limit.
44. The product appears to be used by several people whose identity is not known to the issuer (e.g. the product is used from several IP addresses at the same time).
45. There are frequent changes in the customer's identification data, such as home address, IP address, or linked bank accounts.
46. The product is not used for the purpose it was designed for, for example it is used overseas when it was designed as a shopping centre gift card.

The following factor may contribute to reducing risk:

47. The product is available only to certain categories of customers, for example social benefit recipients or members of staff of a company that issues them to cover employee benefits.

Distribution channel risk factors

The following factors may contribute to increasing risk:

48. Online and non-face-to-face distribution without adequate safeguards, such as electronic signatures, electronic identification documents meeting the criteria set out in Regulation (EU) No 910/2014, and anti-impersonation fraud measures.
49. Distribution through intermediaries that are not themselves obliged service providers under the AML Act or national legislation, where the e-money issuer: relies on the intermediary to fulfil some of the AML/CFT obligations of the e-money issuer; and has not satisfied itself that the intermediary has adequate AML/CFT systems and controls in place.
50. Segmentation of services, that is, the provision of e-money services by several operationally independent service providers without due oversight and coordination.

Country or geographical risk factors

The following factors may contribute to increasing risk:

51. The payee is located in, or the product receives funds from sources in, a country associated with higher ML/TF risk. Supervised institutions should pay particular attention to countries known to provide funding or support for terrorist activities or where groups committing terrorist offences are known to be operating, and countries subject to financial sanctions, embargoes or measures that are related to terrorism, terrorist financing or the proliferation of weapons of mass destruction.

Risks factors

Product, service and transaction risk factors

The following factors may contribute to increasing risk:

52. The product allows high-value or unlimited-value transactions;
53. The product or service has a global reach;
54. The transaction is cash-based or funded with anonymous electronic money, including electronic money covered by Section 15 (3)–(4) of the AML Act;
55. Transfers are made from one or more payers in different countries to a local payee.

The following factor may contribute to reducing risk:

56. The funds used in the transfer come from an account held in the payer's name at an EEA credit or financial institution.

Customer risk factors

The following factors may contribute to increasing risk:

57. The customer's business activity: the customer owns or operates a business that handles large amounts of cash, or the customer's business has a complicated ownership structure.
58. The customer's behaviour: the customer's needs may be better serviced elsewhere, for example because the money remitter is not local to the customer or the customer's business. The customer appears to be acting for someone else, for example others watch over the customer or are visible outside the place where the transaction is made, or the customer reads instructions from a note. The customer's behaviour makes no apparent economic sense, for example the customer accepts a poor exchange rate or high charges unquestioningly, requests a transaction in a currency that is not official tender or commonly used in the country where the customer and/or recipient is located, or requests or provides large amounts of currency in either low or high denominations. The customer's transactions are always just below applicable thresholds, including the customer due diligence threshold for occasional transactions specified in Section 6(1)b) of the AML Act. Supervised institutions should note that the threshold in Article 5(2) of Regulation (EU) 2015/847 of the European Parliament and of the Council of 20 May 2015 on information accompanying transfers of funds and repealing Regulation (EC) No 1781/2006 applies only to transactions that are not funded by cash or anonymous electronic money. The customer's use of the service is unusual, for example it sends or receives money to or from itself or sends funds on immediately after receiving them. The customer appears to know little or is reluctant to provide information about the payee. Several of the supervised institution's customers transfer funds to the same payee, or several customers appear to have the same identification information, for example their address or telephone number. An incoming transaction is not accompanied by the required information on the payer or payee. The amount sent or received is at odds with the customer's income (if known).

The following factors may contribute to reducing risk:

Risk factors associated with institutions providing money transfer services

59. The customer is a long-standing customer of the supervised institution, whose past behaviour has not given rise to suspicion and there are no indications that the ML/TF risk might be increased.
60. The amount transferred is low; however, supervised institutions should note that low amounts alone will not be enough to discount TF risk.

Distribution channel risk factors

The following factors may contribute to increasing risk:

61. There are no restrictions on the funding instrument, for example in the case of cash or payments from e-money products that benefit from the exemption in Section 15(3)–(4) of the AML Act, wire transfers or cheques.
62. The distribution channel used provides a degree of anonymity.
63. The service is provided entirely online without adequate safeguards.
64. The money remittance service is provided through agents that: represent more than one principal; have unusual turnover patterns compared with other agents in similar locations, for example unusually high or low transaction numbers, unusually large cash transactions or a high number of transactions that fall just under the threshold, or undertake business outside normal business hours; undertake a large proportion of business with payers or payees from countries associated with higher ML/TF risk; appear to be unsure about, or inconsistent in, the application of group-wide AML/CFT policies; or are not from the financial sector and conduct another business as their main business.
65. The money remittance service is provided through a large network of agents in different countries.
66. The money remittance service is provided through an overly complex payment chain, for example with a large number of intermediaries operating in different countries or by using untraceable (formal and informal) settlement systems.

The following factors may contribute to reducing risk:

67. Agents are themselves regulated financial institutions.
68. The service can be funded only by transfers from an account held in the customer's name at an EEA credit or financial institution, or from an account over which the customer can be shown to have control.

Country or geographical risk factors

The following factors may contribute to increasing risk:

69. The payer or the payee is located in a country associated with higher ML/TF risk.
70. The payee is resident in a country that has no, or a less developed, formal banking sector, which means that informal money remittance services, such as hawala, may be used at the point of payment.

Risk factors associated with institutions providing asset management services

Risks factors

Product, service and transaction risk factors

The following factors may contribute to increasing risk:

71. Customers requesting large amounts of cash or other physical stores of value such as precious metals;
72. Very high-value transactions;
73. Financial arrangements involving countries associated with higher ML/TF risk (supervised institutions should pay particular attention to countries that have a culture of banking secrecy or do not comply with international tax transparency standards);
74. Lending (including mortgages) secured against the value of assets in other countries, particularly countries where it is difficult to ascertain whether the customer has legitimate title to the collateral, or where the identities of parties guaranteeing the loan are hard to verify;
75. The use of complex business structures such as trusts and private investment vehicles, particularly where the identity of the ultimate beneficial owner may be unclear;
76. Business taking place across multiple countries, particularly where it involves multiple providers of financial services;
77. Cross-border arrangements, where assets are deposited or managed in another financial institution, either of the same financial group or outside of the group, particularly where the other financial institution is based in a country associated with higher ML/TF risk. Supervised institutions should pay particular attention to countries with higher levels of predicate offences, a weak AML/CFT regime or weak tax transparency standards.

Customer risk factors

The following factors may contribute to increasing risk:

78. According to the nature of the customer and the beneficial owner:
    a. Customers with income and/or wealth from high-risk sectors such as the arms industry, the extractive industries, construction, gambling or private military contractors;
    b. Customers about whom credible allegations of wrongdoing have been made;
    c. Customers who expect unusually high levels of confidentiality or discretion;
    d. Customers whose spending or transactional behaviour makes it difficult to establish 'normal', or expected patterns of behaviour;
    e. Very wealthy and influential customers, including customers with a high public profile, non-resident customers and politically exposed persons. Where a customer or a customer's beneficial owner is a politically exposed person, supervised institutions must always apply enhanced due diligence measures in line with Section 19 of the AML Act;

f. The customer requests the supervised institution to facilitate the customer being provided with a product or service by a third party, without a clear business or economic rationale;

Country or geographical risk factors

The following factors may contribute to increasing risk:

79. Business is conducted in countries that have a culture of banking secrecy or do not comply with international tax transparency standards;
80. The customer lives in, or its funds derive from activity in, a country associated with higher ML/TF risk.

Risk factors associated with trade finance providers

Risks factors

81. Banks party to trade finance transactions often have access only to partial information about the transaction and the parties to it. Trade documentation can be diverse and banks may not have expert knowledge of the different types of trade documentation they receive. This can make the identification and assessment of ML/TF risk challenging.
82. Banks should, nevertheless, use common sense and professional judgement to assess the extent to which the information and documentation they have could give rise to concern or suspicion of ML/TF.
83. To the extent possible, banks should consider the following risk factors:

Transaction risk factors

The following factors may contribute to increasing risk:

84. The transaction is unusually large given what is known about the customer's previous trading activity.
    a. The transaction is highly structured, fragmented or complex, involving multiple parties, without apparent legitimate justification.
    b. Copy documents are used in situations where original documentation would be expected, without reasonable explanation.
    c. There are significant discrepancies in documentation, for example between the description of goods in key documents (i.e. invoices and transport documents) and actual goods shipped, to the extent that this is known.
    d. The type, quantity and value of goods is inconsistent with the bank's knowledge of the buyer's business.
    e. The goods transacted present higher risk of money-laundering, for example in the case of certain commodities the prices of which can fluctuate significantly, which can make false prices difficult to detect.
    f. The goods transacted require export licences.
    g. The trade documentation does not comply with applicable laws or standards. Unit prices appear unusual, based on what the bank knows about the goods and trade.
    h. The transaction is otherwise unusual, for example LCs are frequently amended without a clear rationale, or goods are shipped through another country for no apparent commercial reason.

The following factors may contribute to reducing risk:

85. Independent inspection agents have verified the quality and quantity of the goods.
86. Transactions involve established counterparties that have a proven track record of transacting with each other, and due diligence has previously been carried out on them.

Customer risk factors

The following factors may contribute to increasing risk:

87. The transaction and/or the parties involved are out of line with what the bank knows about the customer's previous activity or line of business (e.g. the goods being shipped or the shipping volumes are inconsistent with what is known about the importer's or exporter's business).
88. There are indications that the buyer and seller may be colluding, for example: the buyer and seller are controlled by the same person; transacting businesses have the same address, provide only a registered agent's address, or have other address inconsistencies; the buyer is willing or keen to accept or waive discrepancies in the documentation.
89. The customer is unable or reluctant to provide relevant documentation to support the transaction.
90. The buyer uses agents or third parties.

The following factors may contribute to reducing risk:

91. The customer is an existing customer whose business is well known to the bank and the transaction is in line with that business.
92. The customer is listed on a stock exchange with disclosure requirements similar to the EU's.

Country or geographical risk factors

The following factors may contribute to increasing risk:

93. A country associated with the transaction (including the country where the goods originated from, the country where they are destined for, or the country they transited through, or the country where either party to the transaction is based) has currency exchange controls in place. This increases the risk that the transaction's true purpose is to export currency in contravention of local law.

94. The country associated with the transaction has higher levels of predicate offences (e.g. those related to drug trafficking, smuggling or counterfeiting) or free trade zones.

The following factors may contribute to reducing risk:

95. The trade is within the EU/EEA.
96. The countries associated with the transaction have an AML/CFT regime not less robust than that required under the AML Act, and are associated with low levels of predicate offences.

Risk factors associated with institutions providing life insurance services

Risks factors

Product, service and transaction risk factors

The following factors may contribute to increasing risk:

97. Flexibility of payments, for example the product allows the following: payments from unidentified third parties; high-value or unlimited-value premium payments, overpayments or large volumes of lower value premium payments; and cash payments.
98. Easy access to accumulated funds, for example the product allows partial withdrawals or early surrender at any time, with limited charges or fees.
99. Negotiability, for example the product can be: traded on a secondary market; used as collateral for a loan.
100. Anonymity; the product facilitates or allows the anonymity of the customer.

The following factors may contribute to reducing risk:

The product:

101. only pays out against a pre-defined event, for example death, or on a specific date, such as in the case of credit life insurance policies covering consumer and mortgage loans and paying out only on death of the insured person;
    a. has no surrender value;
    b. has no investment element;
    c. has no third party payment facility;
    d. requires that total investment is curtailed at a low value;
    e. is a life insurance policy where the premium is low;
    f. only allows small-value regular premium payments, for example no overpayment;
    g. is accessible only through employers – for example a pension, superannuation or similar scheme that provides retirement benefits to employees – where contributions are made by way of deduction from wages and the scheme rules do not permit the assignment of a member's interest under the scheme;
    h. cannot be redeemed in the short or medium term, for example in the case of pension schemes without an early surrender option;
    i. cannot be used as collateral;
    j. does not allow cash payments;
    k. has conditions that must be met to benefit from tax relief.

Customer and beneficiary risk factors

The following factors may contribute to increasing risk:

102. The nature of the customer, for example: legal persons whose structure makes it difficult to identify the beneficial owner; the customer or the beneficial owner of the customer is a politically exposed person;

103. The beneficiary of the policy or the beneficial owner of this beneficiary is a politically exposed person; the customer's age is unusual for the type of product sought (e.g. the customer is very young or very old);
104. The contract does not match the customer's wealth situation; the customer's profession or activities are regarded as particularly likely to be related to money laundering, for example because they are known to be very
cash intensive or exposed to a high risk of corruption; the contract is signed by a 'gatekeeper', such as a fiduciary company, acting on behalf of the customer; the policy holder and/or the beneficiary of the contract is a company with nominee shareholders or bearer shares.
105. The customer's behaviour in relation to the contract: the customer frequently transfers the contract to another insurer; frequent and unexplained surrenders, especially when the refund is done to different bank accounts; the customer makes frequent or unexpected use of provisions relating to free cancellation or cooling-off periods, in particular where the refund is made to an apparently unrelated third party; the customer incurs high costs by seeking early termination of a product; the customer transfers the contract to an apparently unrelated third party; the customer's request to change or increase the sum insured and/or the premium payment is unusual or excessive.
106. The customer's behaviour in relation to the beneficiary: the insurer is made aware of a change in the beneficiary only when the claim is made; the customer changes the beneficiary clause and nominates an apparently unrelated third party; the insurer, the customer, the beneficial owner, the beneficiary or the beneficial owner of the beneficiary are in different countries.
107. The customer's behaviour in relation to payments: the customer uses unusual payment methods, such as cash or structured monetary instruments or other payment instruments fostering anonymity; payments from different bank accounts without explanation; payments from banks that are not established in the customer's country of residence; the customer makes frequent or high-value overpayments where this is not expected; payments received from unrelated third parties; catch-up contribution to a retirement plan close to retirement date.

The following factors may contribute to reducing risk:

108. In the case of corporate-owned life insurance, the customer is:
109. a credit or financial institution that is subject to AML/CFT requirements and supervised for compliance with these requirements in a manner that is consistent with the AML Act;
110. a public company listed on a stock exchange and subject to regulatory disclosure requirements (either by stock exchange rules or through law or enforceable means) that impose requirements to ensure adequate transparency of beneficial ownership, or a majority-owned subsidiary of such a company;
111. a public administration or a public enterprise in an EEA state.

Distribution channel risk factors

112. The following factors may contribute to increasing risk: Non-face-to-face sales, such as online, postal or telephone sales, without adequate safeguards, such as electronic signatures or electronic identification documents that comply with 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;
113. Long chains of intermediaries;
114. An intermediary is used in unusual circumstances (e.g. from an unexplained geographical distance).

The following factors may contribute to reducing risk:

115. Intermediaries are well known to the insurer, who is satisfied that the intermediary applies customer due diligence measures commensurate to the risk associated with the relationship and in line with those required
under the AML Act.
116. The product is only available to employees of certain companies that have a contract with the insurer to provide life insurance for their employees, for example as part of a benefits package.

Country or geographical risk factors

The following factors may contribute to increasing risk:

117. The insurer, the customer, the beneficial owner, the beneficiary or the beneficial owner of the beneficiary are based in, or associated with, countries associated with higher ML/TF risk. Supervised institutions should pay particular attention to countries without effective AML/CFT supervision.
118. Premiums are paid through accounts held with financial institutions established in countries associated with higher ML/TF risk. Supervised institutions should pay particular attention to countries without effective AML/CFT supervision.
119. The intermediary is based in, or associated with, a country associated with higher ML/TF risk. Supervised institutions should pay particular attention to countries without effective AML/CFT supervision.

The following factors may contribute to reducing risk:

120. Countries are identified by credible sources, such as mutual evaluations or detailed assessment reports, as having effective AML/CFT systems.
121. The country is identified by credible sources as having a low level of corruption and other criminal activity.

Risk factors associated with investment firms

Risks factors

Product, service and transaction risk factors

The following factors may contribute to increasing risk:

122. Transactions are unusually large;
123. Third party payments are possible;
124. The product or service is used for subscriptions that are quickly followed by redemption possibilities, with limited intervention by the investment manager.

Customer risk factors

The following factors may contribute to increasing risk:

125. The customer's behaviour, for example:
    a. The rationale for the investment lacks an obvious economic purpose;
    b. The customer asks to repurchase or redeem a long-term investment within a short period after the initial investment or before the payout date without a clear rationale, in particular where

this results in financial loss or payment of high transaction fees;

c. The customer requests the repeated purchase and sale of shares within a short period of time without an obvious strategy or economic rationale;
d. Unwillingness to provide customer due diligence information on the customer and the beneficial owner;
e. Frequent changes to customer due diligence information or payment details;
f. The customer transfers funds in excess of those required for the investment and asks for surplus amounts
   to be reimbursed;
g. The circumstances in which the customer makes use of the cooling-off period give rise to suspicion; using multiple accounts without previous notification, especially when these accounts are held in multiple or high-risk countries;
h. The customer wishes to structure the relationship in such a way that multiple parties, for example nominee companies, are used in different countries, particularly where these countries are associated with higher ML/TF risk.

126. The customer's nature, for example:
    a. the customer is a company or trust established in a country associated with higher ML/TF risk (supervised institutions should pay particular attention to countries that do not comply effectively with international tax transparency standards);
    b. The customer is an investment vehicle that carries out little or no due diligence on its own customers;
    c. The customer is an unregulated third party investment vehicle;
    d. The customer's ownership and control structure is opaque;
    e. The customer or the beneficial owner is a politically exposed person or holds another prominent position
       that might enable them to abuse their position for private gain;
    f. The customer is a non-regulated nominee company with unknown shareholders.

127. The customer's business, for example the customer's funds are derived from business in sectors that are associated with a high risk of financial crime.

The following factors may contribute to reducing risk:

128. The customer is an institutional investor whose status has been verified by an EEA government agency, for example a government-approved pensions scheme.
129. The customer is a government body of an EEA state.
130. The customer is a financial institution established in an EEA state.

Country or geographical risk factors

The following factors may contribute to increasing risk:

131. The investor or its custodian is based in a country associated with higher ML/TF risk.
132. The funds come from a country associated with higher ML/TF risk.
133. Investment managers are recommended to develop a good understanding of their customers to help them identify suitable investment portfolios. For this, supervised institutions gather information similar to that obtained for AML/CFT purposes.

Risk factors associated with providers of investment funds

Risks factors

Product, service and transaction risk factors

The following factors may contribute to increasing the risk associated with the fund:

134. The fund is designed for a limited number of individuals or family offices, for example a private fund or single investor fund.
135. It is possible to subscribe to the fund and then quickly redeem the investment without the investor incurring significant administrative costs.

136. Units of the fund can be traded without the fund manager being notified at the time of the trade, and as a result of this information about the investor is divided among several subjects (as is the case with closed-ended funds traded on secondary markets).

The following factors may contribute to increasing the risk associated with the subscription:

137. The subscription involves accounts or third parties in multiple countries, in particular where these countries are associated with a high ML/TF risk as defined in the sector-specific guideline of this Recommendation.
138. The subscription involves third party subscribers or payees, in particular where this is unexpected.

The following factors may contribute to reducing the risk associated with the fund:

139. Third party payments are not allowed.
140. The fund is open to small-scale investors only, with investments capped.

Customer risk factors

The following factors may contribute to increasing risk:

141. The customer's behaviour is unusual, for example:
    a. The investment lacks an obvious strategy or economic purpose, or the customer makes investments that are inconsistent with the customer's overall financial situation, where this is known to the fund manager.
    b. The customer asks to repurchase an investment within a short period after the initial investment or before the payout date without a clear rationale, in particular where this results in financial loss or payment of high transaction fees.
    c. The customer requests the repeated purchase and sale of shares within a short period of time without an obvious strategy or economic rationale.
    d. The customer frequently transfers funds in excess of those required for the investment and asks for surplus amounts to be reimbursed.
    e. The customer uses multiple accounts without previous notification, especially when these accounts are held in multiple countries or in countries associated with higher ML/TF risk.
    f. The customer wishes to structure the relationship in such a way that multiple parties, for example non-regulated nominee companies, are used in different countries, particularly where these

countries are associated with higher ML/TF risk.

g. The customer suddenly changes the settlement location without rationale, for example by changing the customer's country of residence.
h. The customer and the beneficial owner are located in different countries, and at least one of these countries is associated with higher ML/TF risk as defined in the general part (Chapter III) of this Recommendation.
i. The beneficial owner's funds have been generated in a country associated with higher ML/TF risk, in particular where the country is associated with higher levels of predicate offences related to ML/TF.

The following factors may contribute to reducing risk:

142. The customer is an institutional investor whose status has been verified by an EEA government agency, for example a government-approved pensions scheme;
143. The customer is a supervised institution in an EEA country or a third country that has AML/CFT requirements that are not less robust than those set out in the AML Act.

Distribution channel risk factors

The following factors may contribute to increasing risk:

144. Unclear or complex distribution channels that limit the fund manager's oversight of its business relationships;
145. The distributor is located in a country associated with higher ML/TF risk as defined in the general part of this Recommendation.

The following factors may contribute to reducing risk:

146. The fund admits only a designated type of low-risk investor, such as supervised institutions investing as a principal (e.g. life insurance undertakings) or corporate pension schemes.
147. The fund can be purchased and redeemed only through a supervised institution, for example a financial intermediary, in an EEA country or a third country that has AML/CFT requirements that are not less robust than those set out in the AML Act.

Country or geographical risk factors

The following factors may contribute to increasing risk:

148. The investors' money was generated in countries associated with higher ML/TF risk, in particular those associated with higher levels of predicate offences related to money laundering.
149. The fund invests in sectors with higher corruption risk (e.g. the extractive industries or the arms trade) in countries identified by credible sources as having significant levels of corruption or other predicate offences related to ML/TF.