BANKA QENDRORE E REPUBLIKËS SË KOSOVËS
CENTRALNA BANKA REPUBLIKE KOSOVA
CENTRAL BANK OF THE REPUBLIC OF KOSOVO

Pursuant to Article 36, paragraph 1, subparagraph 1.17, and Article 65, paragraphs 1 and 2, of Law No. 03/L-209 on Central Bank of the Republic of Kosovo (Official Gazette of the Republic of Kosovo, No. 77/16 August 2010), amended and supplemented by Law No. 05/L -150 on Central Bank of the Republic of Kosovo (Official Gazette of the Republic of Kosovo, No. 10/3 April 2017), Article 85, paragraph 1, of Law No. 04/L-093 on Banks, Microfinance Institutions and Non-Bank Financial Institutions (Official Gazette of the Republic of Kosovo, No. 11/11 May 2012), Article 4 paragraph 3 and Article 129 paragraph 3 of Law No. 05/L-045 on Insurance (Official Gazette of the Republic of Kosovo/No. 38/24 December 2015), Article 23 paragraph 6 as well as Article 66 paragraph 2 of Law No. 05/L-096 on the Prevention of Money Laundering and Combating Terrorist Financing (Official Gazette of the Republic of Kosovo/No. 18/15 June 2016), the Executive Board of the Central Bank of the Republic of Kosovo, at the meeting held on 29 December 2023, approved the following:

GUIDELINE ON CUSTOMER DUE DILIGENCE AND FACTORS THAT BANKS AND FINANCIAL INSTITUTIONS SHOULD CONSIDER WHEN ASSESSING THE RISK OF MONEY LAUNDERING AND TERRORISM FINANCING

Article 1

Purpose

1. The purpose of this Guideline is to determine the factors that financial institutions must consider when assessing the risk of money laundering and terrorism financing, as well as the level of implementation of due diligence measures towards the customer in proportion to the identified ML/TF risk.
2. The risk factors defined in this Guideline should not be considered exhaustive, therefore, financial institutions shall, as deemed necessary, take into account other factors when assessing the risk of money laundering and terrorism financing.

Article 2

Scope

This Guideline has been prepared in cooperation and coordination with the Financial Intelligence Unit (FIU-K), and it shall be applied to all banks, non-bank financial institutions, microfinance institutions, insurers and currency exchange offices.

Article 3

Definitions

1. All terms used in this Guideline shall have the same meaning as the terms defined in the Regulation on Prevention of Money Laundering and Financing of Terrorism and/or the definitions below for the purpose of this Guideline.
2. *Financial Institution* – means banks, non-bank financial institutions, microfinance institutions, insurers, pension funds and currency exchange offices.
3. *ML/TF* – Money Laundering and Terrorism Financing
4. *Risk* - means the impact and likelihood of ML/TF occurring. Risk refers to inherent risk, that is, the level of risk that exists before mitigation measures are implemented. It does not refer to residual risk, that is, the level of risk that remains after mitigation.
5. *Inherent risk* – means the inherent risk that exists before mitigation.
6. *Risk Factors* – means variables that alone or in combination can increase or decrease the risk of ML/TF.
7. *CDD* – Customer Due Diligence
8. *EDD* – Enhanced Due Diligence
9. *SDD* – Simplified Due Diligence
10. *PEP*- Politically Exposed Person

Article 4

ML/TF risk assessment

1. Financial institutions must ensure that they have full knowledge of the ML/TF risks to which they are exposed.
2. Financial institutions shall assess the risk from ML/TF to which they are exposed as a result of the nature and complexity of the institution's activity and the assessment of the risk from ML/TF to which they are exposed as a result of entering into business relationships and carrying out occasional transactions.

3. The ML/TF risk assessment shall consist of two separate but interrelated steps:

   3.1 Identification of risk factors from ML/TF

   3.2 ML/TF risk assessment

4. When assessing the overall level of residual ML/TF risk, financial institutions should consider the level of inherent risk and the quality of controls and other risk mitigation factors.

Article 5

Updating the ML/TF risk assessment

1. Financial institutions should put in place systems and controls to ensure that their ML/TF risk assessments remain up-to-date and relevant.
2. Systems and controls to ensure that ML/TF risk assessments remain up-to-date and relevant include:

   2.1. Determination of a date for each calendar year in which the next update of the ML/TF risk assessment is carried out at the level of the institution's activity and at the level of business relations and occasional transactions.

   2.2. Immediate reflection on their ML/TF risk assessments when it is identified that a new ML/TF risk has emerged or an existing risk has increased.

   2.3. Careful recording of all relevant issues or events during the relevant period that may have an impact on the ML/TF risk assessment.

3. Financial institutions should also ensure that they have systems and controls in place to identify emerging ML/TF risks, assess these risks, and where appropriate, in a timely manner incorporate them into the ML/TF risk assessment.

Article 6

ML/TF risk assessment at the level of the institution's activity

1. Risk assessment at the activity level should help financial institutions understand where they are exposed to the risk of ML/TF and which areas of their business they should prioritize in the fight against ML/TF.
2. Financial institutions shall have a complete picture of the ML/TF risks to which they are exposed, identifying and assessing the ML/TF risk related to the products and services they offer, the jurisdictions in which they operate and distribution channels that they use to serve customers.

3. Financial institutions shall ensure that the risk assessment at the level of their activity is in accordance with their business profile and, at the same time, the factors and risks specific to the institution's business shall be taken into account.
4. In cases where the financial institution is part of a group that designs a group-wide risk assessment, the financial institution shall consider whether the group-wide risk assessment is sufficiently specific to reflect the institution's business and the risks to which it is exposed as a result of the group's connections with countries and geographical areas, and if necessary complete the risk assessment within the group. If the group is located in a country that is associated with a high level of corruption, the financial institution must reflect this fact in the risk assessment even if the risk assessment within the group does not reflect this point.
5. A general ML/TF risk assessment that is not tailored to the institution's specific needs and business model or a group-level risk assessment that is applied without question cannot be considered to meet the regulatory and legal criteria in power.
6. The information contained in this Guideline shall be intended to provide a general orientation on risks and their management and shall not replace the legal measures provided for in the Law on PML/CTF and relevant regulations in force.
7. The steps that financial institutions must undertake in identifying and assessing the risk of ML/TF must be in proportion to the nature and size of the institution. Small institutions that do not offer complex products or services and that have limited or only local exposure may not need a complex or sophisticated risk assessment.
8. The financial institution should take the necessary steps to ensure that all staff understand the ML/TF risk assessment and its impact on their work.
9. The financial institution shall inform and provide sufficient information to senior management regarding the results of the risk assessment and the level of risk exposed.

Article 7

ML/TF risk assessment at the level of business relationships

1. Financial institutions shall identify which ML/TF risks they are exposed to as a result of entering into or maintaining a business relationship or carrying out an occasional transaction.
2. Financial institutions, when identifying the risk from ML/TF related to business relationships or occasional transactions, should consider relevant risk factors including who their customer is, the countries or geographic areas where they operate, the products, services and transactions the customer requires as well as the distribution channels for these products, services and transactions.

3. Financial institutions, before entering into business relationships or carrying out occasional transactions, in accordance with the relevant legal and regulatory requirements in force, must apply due diligence measures to the customer which at least include:

   3.1 Identification of the customer and, in cases where required, the beneficial owner;

   3.2 Customer verification based on reliable and independent sources and, where applicable, verification of the identity of the beneficial owner;

   3.3 Determination of the purpose and nature of the business relationship.

4. Financial institutions shall adjust the level of implementation of initial risk-based customer due diligence measures taking into account the findings from the business-wide risk assessment. In cases where the risk associated with a business relationship is likely to be low, institutions may apply simplified customer due diligence. Whereas in cases where the risk related to a business relationship is likely to enhance, institutions must apply enhanced due diligence measures.

5. Financial institutions shall collect sufficient information in order to identify all relevant risk factors at the beginning or during the business relationship or before the execution of the occasional transactions.

Article 8

Identification of risk factors of ML/TF

1. Financial institutions shall identify risk factors related to their customers, countries or geographical areas, products and services, and distribution channels.

2. For the purposes of paragraph 1 of this Article, financial institutions shall take into account, and not be limited to, the following data sources:

   2.1. National and international ML/TF risk assessments;

   2.2. Laws, Regulations, Instructions as well as other relevant documents issued by the competent authorities in the country;

   2.3. Reports and other information published by the Financial Intelligence Unit and other government authorities competent for criminal prosecution;

   2.4. Information obtained from customer due diligence;

   2.5. Professional knowledge and experience;

Article 9

ML/TF risk factors related to the customer and the beneficial owner

1. The risk factors that can be considered relevant when identifying the risk related to the activity of the customer and the beneficial owner, include but are not limited to:

    1.1. Does the customer or beneficial owner have links to sectors that are usually associated with a higher risk of corruption?

    1.2. Does the customer or beneficial owner have links to sectors that are associated with higher ML/TF risk?

    1.3. Does the customer or beneficial owner have links with sectors involving significant amounts of cash?

    1.4. When the customer is a legal entity, trust, or other type of legal agreement, what is the purpose of their creation? For example, what is the nature of their business?

    1.5. Does the customer have political connections, for example, are they politically exposed persons (PEPs), or is the beneficial owner a PEP? When a customer or beneficial owner is a PEP, the entity must implement enhanced due diligence measures in accordance with Article 22 of the Law on PML/CTF?

    1.6. Does the customer or beneficial owner hold some other prominent position or enjoy a high public reputation that might allow them to abuse this position for private gain?

    1.7. Is the customer a legal entity subject to applicable disclosure rules and requirements that ensure that reliable information about the customer's beneficial owner is publicly available, for example public companies listed on stock exchanges that make such disclosure a condition to be listed?

    1.8. Is the customer a bank or financial institution operating on its own account from a jurisdiction with an effective PML/CTF regime and is it supervised at the local level for compliance with PML/CTF obligations? Is there evidence that the customer has been subject to supervisory sanctions or penalties for non-compliance with PML/CTF obligations or other wider governance requirements in recent years?

    1.9. Is the customer a public institution or enterprise from a jurisdiction with low levels of corruption?

    1.10. Is the knowledge of the customer or beneficial owner consistent with what the reporting entity knows about their past, current or planned business activity, their business turnover, the source of funds and the source of the beneficial owner's wealth?

2. Risk factors that may be considered relevant when identifying risk related to the reputation of the customer and the beneficial owner include but are not limited to:

    2.1. Are there conflicting media reports or other relevant sources of information about the customer, for example are there any allegations of criminality or terrorism against the customer or beneficial owner? If so, are these supported and reliable? Reporting entities must determine the credibility of claims based on the quality and

independence of the data source and the persistence of reporting those claims, among other considerations. Reporting entities should be aware that the absence of criminal convictions alone may not be sufficient to disprove allegations of wrongdoing.

2.2. Is there knowledge that the customer, the beneficial owner or anyone else closely related to them has funds or other assets frozen due to administrative or criminal proceedings or allegations of terrorism or terrorism financing? Does the reporting entity have reason to suspect that the customer or beneficial owner or any other person publicly known to be closely associated with them has at some time in the past been subject to such freezing of funds or assets?

2.3. Does the reporting entity know whether the customer or beneficial owner has been the subject of a suspicious transaction report in the past?

2.4. Does the reporting entity have any inside information about the integrity of the customer or beneficial owner, obtained, for example, during a long business relationship?

3. The following risk factors may be relevant when considering the risk associated with the nature and behaviour of the customer or beneficial owner; financial institutions must consider the fact that not all of these risk factors are apparent from the outset; these factors may appear only after the business relationship has been established:

3.1. Does the customer have legitimate reasons that made it impossible for him to provide strong convincing evidence of his identity?

3.2. Does the reporting entity have doubts about the authenticity or accuracy of the identity of the customer or beneficial owner?

3.3. Are there indications that the customer made efforts to avoid establishing the business relationship? For example, is the customer looking to carry out a one-way transaction or several transactions when in such situations establishing a business relationship may make more economic sense?

3.4. Is the customer ownership and control structure transparent and meaningful? If the customer's ownership and control structure is complex or opaque, is there an obvious commercial or legal rationale?

3.5. Does the customer issue bearer shares or have nominee shareholders?

3.6. Is the customer a legal entity or legal agreement that can be used as a holder of funds or assets?

3.7. Is there compelling reason for changes in the customer's ownership and control structure?

3.8. Does the customer require transactions that are complex in nature, unexplained, unusually large, or have an unusual or unexpected pattern without an apparent economic

or legal purpose or sound commercial rationale? Is there reason to suspect that the customer is trying to avoid specific thresholds such as those set out in the Law on PML/CTF, where applicable?

3.9. Does the customer require unnecessary or unreasonable levels of confidentiality? For example, is the customer willing to share CDD information, or does it appear to want to mask the true nature of its business?

3.10. Can the source of the customer's or beneficial owner's wealth and funds be readily explained, for example through employment, inheritance or investments? Is the explanation reasonable?

3.11. Does the customer use the products and services they received as expected when the business relationship was established?

3.12. When the customer is non-resident, is there a sound economic and legal rationale for the customer seeking this type of financial service?

4. When identifying the risk associated with the nature and behaviour of a customer or beneficial owner, financial institutions should pay particular attention to risk factors that, although not specific to terrorism financing, may indicate increased TF risk, especially in situations where other TF risk factors are also present. For this purpose, financial institutions must take into account at least the following risk factors:

4.1. Is the customer or beneficial owner a person included in the lists of persons, groups and entities involved in terrorist acts and subject to restrictive measures, or is known to have close personal or professional ties with persons registered on such lists (for example, because they are in a relationship or otherwise live with such a person)?

4.2. Is the customer or beneficial owner a person who is publicly known to be under investigation for terrorist activity or has been convicted of terrorist activity, or is known to have close personal or professional ties to such a person?

4.3. Does the customer carry out transactions characterized by the transfer of incoming and outgoing funds from and/or to countries where groups that commit terrorist acts are known to operate, are known to be sources of terrorist financing or are subject to international sanctions? If so, can these transfers be easily explained, for example, through family ties or business relationships?

4.4. Is the customer a non-profit organization whose activities or management is publicly associated with extremism or terrorist sympathies; whose transaction behaviour is characterized by large transfers of large amounts of funds to jurisdictions associated with higher ML/TF risks and high-risk third countries?

4.5. Does the customer carry out transactions characterized by large cash flows in a short period of time, involving non-profit organizations with unclear ties (e.g., they are

located in the same physical location; they share the same representatives or employees or hold multiple accounts with the same names)?

Article 10

ML/TF risk factors related to countries and geographical areas

1. When identifying risk factors related to countries and geographical areas, financial institutions should consider the risk associated with:

    1.1. Jurisdictions in which the customer and beneficial owner is located or is resident;

    1.2. Jurisdictions which are the places of operation of customers and beneficial owners; and

    1.3. Jurisdictions in which the customer and the beneficial owner have relevant personal, business, financial ties or legal interests.

2. Financial institutions should note that the nature and scope of the business relationship, or type of business, often determines the relative importance of individual country and geographical risk factors. For example:

    2.1. When funds used in business dealings are generated abroad, the level of criminal offenses related to money laundering and the effectiveness of the country's legal system are particularly important.

    2.2. When funds are received in, or sent to, jurisdictions where terrorist groups are known to operate, financial institutions should consider the extent to which this may be expected or may raise suspicion, based on what the financial institution knows about the intent and the nature of the business relationship.

    2.3. When the customer is a bank or financial institution, reporting entities should pay particular attention to the country's appropriate PML/CTF regime and the effectiveness of PML/CTF supervision.

    2.4. When the customer is a legal person or trust, financial institutions should consider the extent to which the country where the customer and, where applicable, the beneficial owner are registered, effectively meets international tax transparency standards.

3. Risk factors that financial institutions should consider when identifying the effectiveness of a jurisdiction's PML/CTF regime include:

    3.1. Has the country identified strategic deficiencies in its PML/CTF regime?

    3.2. Does the country's legislation prohibit the implementation of policies and procedures at the group level?

    3.3. Is there any information from more than one reliable and credible source about the quality of the jurisdiction's PML/CTF control, including information about the

quality and effectiveness of regulatory supervision and assessment? Examples of possible sources include mutual assessment reports from the Financial Action Task Force (FATF) or FATF-style regional bodies (FSRBs) (a good starting point is the executive summary and key findings and assessment of compliance with Recommendations 10, 26 and 27 and Immediate Outcomes 3 and 4), FATF's list of high risk and non-cooperative countries, International Monetary Fund (IMF) and Financial Sector Assessment Program (FSAP) assessments. Financial institutions should note that membership of FATF or FSRB (e.g., Moneyval) does not mean that the jurisdiction's PML/CTF regime is adequate and effective.

4. Risk factors that financial institutions should consider when identifying the level of terrorism financing risk associated with a jurisdiction include:

    4.1. Is there any information, for example from law enforcement authorities or reliable and credible open media sources, suggesting that a jurisdiction provides funding or support for terrorist activities or that groups committing terrorist offenses are known to operate in that country or territory?

    4.2. Is the jurisdiction subject to financial sanctions, embargoes or measures relating to terrorism, terrorism financing or proliferation expansion, for example, by the United Nations or the European Union?

5. Risk factors that financial institutions should consider when identifying a jurisdiction's level of transparency and compliance in the area of taxation include:

    5.1. Is there any information from more than one reliable and credible source that the country is considered compliant with international tax transparency and information exchange standards? Is there evidence that the relevant rules are effectively implemented in practice? Examples of possible sources include reports from the Global Forum on Transparency and Exchange of Information for Tax Purposes of the Organization for Economic Co-operation and Development (OECD), which assess jurisdictions for tax transparency and information exchange purposes; assessments of jurisdictional committees for 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 FATF or FSRB; and IMF assessments (e.g., IMF staff assessments of financial centres operating in offshore countries).

    5.2. Has the jurisdiction committed to, and effectively implemented, the Common Reporting Standard for Automatic Exchange of Information, which was adopted by the G20 in 2014?

    5.3. Has the jurisdiction established reliable and accessible registers of beneficial ownership?

6. Risk factors that financial institutions should consider when identifying the risk associated with the level of money laundering offenses include:

   6.1. Is there any information from credible and reliable public sources about the level of criminal offenses related to money laundering, for example corruption, organized crime, tax offenses and fraud? Examples include corruption perception indices; OECD progress reports on the implementation of the OECD anti-bribery convention; and United Nations Office on Drugs and Crime - World Drug Report.

   6.2. Is there any information from more than one reliable and credible source about the ability of the jurisdiction's investigative and judicial system to effectively investigate and prosecute these crimes?

Article 11

ML/TF risk factors related to products, services and transactions

1. When identifying risk factors related to products, services and transactions, financial institutions should consider the risk associated with:

   1.1. the level of transparency of the product, service or transaction that may be provided;

   1.2. the complexity of the product, service or transaction; and

   1.3. the value or size of the product, service or transaction.

2. Risk factors that financial institutions should consider when identifying the risk associated with the transparency of a product, service or transaction include:

   2.1. To what extent do the products or services allow the customer, beneficial owner or beneficial ownership structures to remain anonymous, or facilitate the concealment of their identity? Examples of such products and services include bearer shares, trust deposits, offshore legal entities, certain trusts, and legal entities such as foundations that can be structured to benefit from anonymity and allow relations with shell companies or company with nominated shareholders.

   2.2. To what extent is it possible for a third party who is not part of the business relationship to give instructions, for example in the case of certain correspondent bank relationships?

3. Risk factors that financial institutions shall consider when identifying the risk associated with the complexity of a product, service or transaction include:

   3.1. How complex is the transaction and does it involve multiple parties or multiple jurisdictions, for example in the case of certain commercial business transactions?

   3.2. To what extent do products or services allow third-party payments or accept overpayments where not normally expected? Where third party payment is expected, does the financial institution know the identity of the third party, for example is it a

beneficiary state authority or a guarantor? Or are the products and services financed exclusively by transfers of funds from the customer's own account to another financial institution subject to PML/CTF standards and supervision?

3.3. Does the financial institution understand the risks associated with its new or innovative product or service, especially when it involves the use of new payment technologies or methods?

4. Risk factors that financial institutions should consider when identifying the risk associated with the value or size of a product, service or transaction include:

4.1. To what extent do products or services support the use of cash, such as many payment services but also certain current accounts?

4.2. To what extent do products or services encourage or facilitate high-value transactions? Are there any restrictions on transaction values or premium levels that may limit the use of the product or service for ML/TF purposes?

Article 12

PML/CTF risk factors related to distribution channels

1. When identifying risk factors related to distribution channels, financial institutions should consider the risk associated with:

1.1. the extent to which the business relationship is carried out without physical presence;

1.2. the application of third parties or intermediaries.

2. When assessing the risk associated with the manner in which the customer receives products or services, financial institutions must consider a number of factors including:

2.1. If the customer is physically present for identification purposes. If not, has the financial institution applied a reliable form of CDD without physical presence? Are steps taken to prevent forgery or identity fraud?

2.2. If the customer is identified by third parties, the factors to be considered are:

2.2.1. If the third party applies the measures of the CDD, stores and maintains the data according to the legal requirements in force, is supervised for compliance with PML/CTF as well as if there are indications for the third party that the level of compliance with PML/CTF is inadequate or if it has been subject to administrative measures for violation of PML/CTF obligations.

2.2.2. If the third party comes from high ML/TF risk jurisdictions.

2.2.3. Financial institutions must ensure that the third party provides identification or verification documents in time upon request; the

quality of CDD measures is acceptable; the level of CDD applied by the third party is in accordance with the risk from ML/TF.

2.3. If the customer is identified through a related agent, i.e., without direct contact of the financial institution, to what extent can the financial institution be convinced that the agent has obtained sufficient information to ensure that the financial institution knows its customer and the level of risk related to business relationships.

Article 13

ML/TF risk assessment

1. Financial institutions should have a holistic view of the ML/TF risk factors they have identified, which together determine the level of ML/TF risk associated with a business relationship, a random transaction or their own business.
2. Financial institutions, when assessing ML/TF risk, may weight factors depending on their relative importance.
3. When assessing risk factors, an informed judgment must be made regarding the significance of the various risk factors in the context of the business relationship or the particular transaction.
4. The importance given to each of the factors is likely to vary from product to product and from customer to customer (or category of customer) as well as from one institution to another. When assessing risk factors, financial institutions should ensure that:
    4.1. The assessment must not be unduly influenced by only one factor;
    4.2. Economic or profit assessments do not affect the risk assessment;
    4.3. The assessment does not lead to a situation where it is impossible for any business relationship to be classified as high risk;
    4.4. Legal provisions regarding situations that always present a high risk of money laundering cannot be overridden by the assessments of financial institutions.
5. When the financial institution uses automated IT systems to share aggregate risk scores to categorize business relationships or occasional transactions and does not develop them itself but buys them from an external provider, it must understand how the system works and how the risk factors combine to achieve the overall risk score. The financial institution must always be able to convince itself that the results obtained reflect an understanding of the ML/TF risk and must be able to demonstrate this to the competent authority.

Article 14

Risk categorization

1. Financial institutions must decide on the most appropriate way to categorize risk. This depends on the nature and size of the business and the types of ML/TF risk it is exposed to. Although institutions often categorize risk as high, medium, and low, other categorizations are possible.
2. After assessing the risk, and taking into account both the inherent risks and the mitigating measures it has identified, the institution should categorize its lines of business, as well as their business relationships and occasional transactions according to the perceived level of ML/TF risk.

Article 15

Customer Due Diligence Measures applicable to all financial institutions

1. Risk assessments should help the financial institution identify where it should focus its ML/TF risk management efforts, both at customer onboarding and over the life of the business relationship.
2. Financial institutions should ensure that their PML/CTF policies and procedures are based on and reflect their risk assessment.
3. Financial institutions should also ensure that their PML/CTF policies and procedures are readily available, applied, effective and understood by all relevant staff.
4. When fulfilling their obligation to obtain senior management approval of their PML/CTF policies, controls and procedures, financial institutions should ensure that senior management has access to sufficient data, including risk assessment by ML/TF, in order to be informed about the adequacy and effectiveness of these policies and procedures and in particular about the measures of the CDD.

Article 16

Customer Due Diligence

1. Due diligence measures should help financial institutions better understand the risk associated with individual business relationships and occasional transactions.
2. As part of this, financial institutions must implement each of the measures for CDD defined in the provisions of the Law on PML/CTF, but can determine the extent of these measures also on the basis of risk sensitivity.
3. Financial institutions should clearly define in their policies and procedures:
    3.1. Who is the customer and, where applicable, the beneficial owner for each type of customer and category of products and services, and whose identity must be verified for CDD purposes?

3.2. What constitutes an occasional transaction in the context of their business, and at what point a series of one-off transactions constitutes a business relationship, rather than an occasional transaction, taking into account factors such as the frequency or regularity with which the customer returns for random transactions and the extent to which the relationship is expected to have, or appear to have, an element of duration. Financial institutions should take into account that the monetary limit determined according to the legal provisions in force is important only to the extent that it causes an absolute requirement to implement the CDD measures; a series of occasional transactions may constitute a business relationship even when this threshold is not met;

3.3. How to verify the identity of the customer and, where applicable, of the beneficial owner and how they expect the nature and purpose of the business relationship to be established;

3.4. What level of monitoring applies and under what circumstances;

3.5. Risk appetite of the financial institution.

4. Financial institutions must be able to demonstrate to their supervisory authority that the CDD measures they have applied are consistent with ML/TF risks.

Article 17

Simplified Customer Due Diligence

1. To the extent permitted by local legislation, financial institutions may apply simplified due diligence measures in situations where the ML/TF risk associated with business relationships has been assessed as low. Simplified due diligence is not an exception to any of the measures of the CDD; however, financial institutions may adjust the volume, timing or type of any or all CDD measures in a manner consistent with the low risk they have identified.

2. Simplified customer due diligence measures that financial institutions may apply include, but are not limited to:

    2.1. Adapting the timing of the CDD, for example when the requested product or transaction has features that limit its use for ML/TF purposes, for example by:

        2.1.1. verifying the identity of the customer or the beneficial owner during the establishment of the business relationship; or

        2.1.2. verifying the identity of the customer or beneficial owner after transactions pass a specified threshold or after a reasonable time limit (as determined by applicable law) has passed. Financial institutions must ensure that:

2.1.2.1. this does not result in a de facto exemption from the CDD, that is, financial institutions must ensure that the identity of the customer or beneficial owner is ultimately verified;

2.1.2.2. the threshold or time limit is set at a reasonably low level (although, in relation to terrorism financing, financial institutions should consider that the low threshold alone may not be sufficient to reduce the risk);

2.1.2.3. they have systems in place to detect when a threshold or deadline has been reached; and

2.1.2.4. they do not ignore CDD or delay obtaining relevant information about the customer, when the legislation in force requires that this information be obtained first.

2.1.3. Tailoring the amount of information received for identification, verification or monitoring purposes, for example by:

2.1.3.1. verifying the identity based on information obtained from a credible, reliable and independent document or data source only; or

2.1.3.2. claiming the nature and purpose of the business relationship because the product is designed for a particular use only, such as a company pension scheme or shopping centre gift cards.

2.1.4. Adapting the quality or source of information received for identification, verification or monitoring purposes, for example by:

2.1.4.1. prioritizing information received from the customer in advance over an independent source when verifying the identity of the beneficial owner; or

2.1.4.2. where the risk associated with all aspects of the relationship is very low, relying on the source of the funds to meet some of the requirements of the CDD, for example where the funds are benefit payments from the state or where the funds are transferred from an account in the name of the customer from the reporting entity from the European Economic Area.

2.1.5. Adjusting the frequency and intensity of transaction monitoring, for example by only monitoring transactions above a certain threshold. Where financial institutions choose to do so, they must ensure that the threshold is set at a reasonable level and that they have systems in place to identify related transactions which, together, exceed that threshold.

3. The information that the financial institution obtains when applying the SDD measures should enable the financial institution to be reasonably convinced that its assessment of the risk associated with the relationship is low and is reasonable. It must also be sufficient to provide the financial institution with sufficient information about the nature of the business relationship to identify any unusual or suspicious transactions. The application of simplified due diligence does not exempt a financial institution from reporting suspicious transactions to FIU-K.

Article 18

Enhanced Customer Due Diligence

1. Financial institutions should apply enhanced due diligence measures in higher risk situations to manage and mitigate those risks appropriately. The enhanced due diligence measures cannot be substituted for the regular CDD measures, but must be implemented in addition to the regular CDD measures.
2. Specific cases that financial institutions should always treat as high risk may include:
    2.1. where the customer, or the beneficial owner of the customer, is a PEP;
    2.2. where the financial institution deals with natural persons or legal entities located in high-risk third countries;
    2.3. regarding correspondent relations with respondent banks from third countries;
    2.4. all transactions which are:
        2.4.1. complex;
        2.4.2. extremely large;
        2.4.3. carried out in an unusual form or:
        2.4.4. that do not have any obvious economic or legal purpose.
3. Financial institutions must implement the EDD measures in those situations where this is proportional to the ML/TF risk they have identified.

Article 19

Sector-specific instructions

1. Sector-specific instructions complement the general instructions of this Guideline. Reporting entities should have an overview of the risk associated with the situation and consider that isolated risk factors do not necessarily place a business relationship or transaction in a higher or lower risk category.

Article 20

Instructions for commercial banks

1. Banking institutions must take into account the following risk factors and measures in addition to those defined by this Guideline:

1.1. The following factors may contribute to increased risk from products, services and transactions:

1.1.1. product features that favour anonymity;

1.1.2. the product allows payments from third parties not related to the product or not identified in advance, when such payments are not expected, for example for mortgages or loans;

1.1.3. the product does not impose restrictions on circulation, cross-border transactions or similar features of the product;

1.1.4. new products and new business practices, including new delivery mechanisms, and the use of new or emerging technologies for new and existing products where these are not yet well understood;

1.1.5. lending (including mortgages) secured against the value of assets in other jurisdictions, particularly countries where it is difficult to ascertain whether the customer has legal title to the collateral, or where the identity of the parties guaranteeing the loan is difficult to verify;

1.1.6. unusually high volume or large value of transactions.

1.2. The following factors can contribute to reducing the risk of products, services and transactions:

1.2.1. The product has limited features, for example in the following cases:

1.2.1.1. fixed-term savings product with low savings thresholds;

1.2.1.2. product where the benefits cannot be achieved for the benefit of a third party;

1.2.1.3. product where the benefits are achieved only in the long term or for a specific purpose, such as retirement or the purchase of property;

1.2.1.4. low-value loans, including those conditioned on the purchase of a specific consumer good or service; or

1.2.1.5. low-value product, including rentals, where the legal and beneficial title to the funds is not transferred to the customer until the contractual relationship is terminated or may never be transferred.

1.2.2. 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.

1.2.3. Transactions must be conducted through an account in the customer's name at a bank or financial institution subject to PML/CTF requirements according to international standards.

1.2.4. No overpayment facilities are provided.

1.3. The following factors may contribute to increased customer risk:

1.3.1. The nature of the customer, for example:

1.3.1.1. The customer transacts in cash.

1.3.1.2. The customer is an entity associated with a higher level of money laundering risk, for example, gambling businesses.

1.3.1.3. The customer is a related entity with a higher risk of corruption, for example operating in the mineral extraction industries or arms trade.

1.3.1.4. The customer is a non-profit organization that supports related jurisdictions with a high risk of TF.

1.3.1.5. The customer is a new company without a proper business portfolio or past data.

1.3.1.6. The customer is a non-resident.

1.3.1.7. The customer's beneficial owner cannot be easily identified, for example, because the customer's ownership structure is unusual, unnecessarily complicated or obscure.

1.3.2. Customer behaviour, for example:

1.3.2.1. The customer does not wish to appear or provide information to CDD in order to avoid face-to-face contact.

1.3.2.2. Customer identity data is in non-standard form for no apparent reason.

1.3.2.3. The customer's behaviour or transaction volume is not consistent with what is expected of the customer category to which they belong, or is unexpected based on the information the customer provided when opening the account.

1.3.2.4. The customer's behaviour is unusual, for example the customer suddenly and without reasonable explanation accelerates the agreed repayment time, by means of repayment of an amount or early termination; deposits or outgoing payments in high value banknotes for no apparent reason; increases activity after a dormant period; or makes transactions that appear to have no economic rationale.

1.4. The following factors can contribute to reducing the risk from the customer:

1.4.1. The customer is a long-time customer whose previous transactions have not raised doubts or concerns, and the product or service requested is consistent with the customer's risk profile.

1.5. The following factors may contribute to increased country risk or geographic risk.

1.5.1. Customer funds come from business or personal connections in jurisdictions associated with higher ML/TF risk.

1.5.2. The payer is located in a jurisdiction associated with a higher ML/TF risk. Reporting entities should pay particular attention to jurisdictions known to provide funding or support for terrorism activities or where terrorist groups are known to operate, and the jurisdictions are subject to financial sanctions, embargoes or measures related to terrorism, terrorist financing or proliferation.

1.6. The following factors can contribute to reducing country risk and geographic risk:

1.6.1. The countries related to the transaction are part of the jurisdictions that have an PML/CTF regime in compliance with international standards and that have low levels of related criminal offences.

1.7. The following factors may contribute to increased risk from service delivery channels:

1.7.1. Business relations without physical presence, when there are no additional security measures for example electronic signatures, electronic identification certificates in accordance with international standards in this field and when additional data verification controls are missing.

1.7.2. relying on third-party CDD measures in situations where the bank does not have a long-term relationship with the referring third party;

1.7.3. new distribution channels that have not yet been tested.

1.8. The following factors can contribute to reducing risk from service delivery channels:

1.8.1. The product is only available to customers who meet specific eligibility criteria set by local public authorities, such as recipients of state benefits.

2. Where banks use automated systems to identify ML/FT risk associated with individual business relationships or occasional transactions and to identify suspicious transactions, they must ensure that these systems are fit for purpose in accordance with the criteria determined by this Guideline. The use of automated IT systems should never be considered a substitute for due diligence by staff.

2.1. When the risk associated with a business relationship or occasional transaction has increased, banks must apply EDD measures. These may include:

2.1.1. Verifying the identity of the customer and the beneficial owner based on more than one reliable and independent source.

2.1.2. Identifying and verifying the identity of other shareholders who are not the beneficial owner of the customer or any natural person who has the authority to administer accounts or give instructions regarding the transfer of funds or the transfer of securities.

2.1.3. Obtaining more information about the customer and the nature and purpose of the business relationship to build a more complete profile of the customer, for example by conducting media and open-source research. Examples of the type of information banks may request include:

2.1.3.1. the nature of the customer's business or workplace;

2.1.3.2. the source of the customer's assets and the source of the customer's funds involved in the business relationship, to be reasonably convinced that these are legitimate;

2.1.3.3. The purpose of the transaction, including, when appropriate, the destination of the customer's funds;

2.1.3.4. Information about any connection the customer may have with other jurisdictions (headquarters, operational facilities, branches, etc.) and individuals that may affect its operations; or

2.1.3.5. where the customer is located in another country, why they seek services from commercial banks outside their country's jurisdiction.

2.1.4. Increasing the frequency of transaction monitoring.

2.1.5. Reviewing and, where necessary, updating information and documentation held more frequently. When the risk associated with the relationship is particularly high, banks should review the business relationship annually.

2.2. When the risk associated with the business relationship or the occasional transaction is low, banks may apply simplified due diligence measures. These may include:

2.2.1. for customers subject to the statutory licensing and regulator regime, identity must be verified based on evidence that the customer is subject to this regime, for example through a check of the regulator's public register;

2.2.2. accepting alternative forms of identity that meet the independent and reliable source criterion such as a letter from a government agency or other public body trusted by the customer where there are reasonable grounds for the customer not being able to provide standard proof of identity and provided that there is no reason for suspicion;

Article 21

Instructions for correspondence relations

3. Financial institutions must take into account the following risk factors and measures in addition to those defined by this Guideline:

3.1. The following factors may contribute to increased risk from products, services and transactions:

3.1.1. The account may 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 indirectly provides services to other banks that are not respondents.

3.1.2. The account may be used by other entities within the respondent's group that have not been subject to due diligence by the correspondent.

3.1.3. The service includes the opening of accounts payable, which allows the respondent's customers to conduct transactions directly on the respondent's account.

3.2. The following factors can contribute to reducing the risk of products, services and transactions:

3.2.1. The relationship is limited to the capabilities of SWIFT RMA, which is designed to manage communications between financial institutions. In a SWIFT RMA relationship, the respondent or counterparty has no relationship with accounts payable.

3.2.2. Banks act on their own account instead of carrying out transactions on behalf of their customers, for example in the case of foreign exchange services between two banks, and third parties are not involved. In these cases, the transaction is carried out for the respondent bank's own account.

3.2.3. The transaction relates to the sale, purchase or holding of securities on regulated markets.

3.3. The following factors may contribute to increased customer risk:

3.3.1. The respondent's PML/CTF policies and the systems and controls that the respondent applies are not in compliance with international standards and applicable legal requirements.

3.3.2. The respondent is not subject to adequate PML/CTF supervision.

3.3.3. The respondent or the group to which he belongs, has recently been subject to punishment or administrative measures for violation of PML/CTF obligations.

3.3.4. The Respondent conducts significant business with sectors associated with higher levels of ML/TF risk; for example, the respondent conducts remittance business or substantial remittance business on behalf of certain remitters or bureaux de change, with non-residents or in a currency other than that of the country in which it is established.

3.3.5. The respondent's management or ownership includes the PEP, in particular where the PEP may exercise significant influence over the respondent, such that the PEP's reputation, integrity or suitability as a board member or key office holder raises concerns, or where the PEP is from a jurisdiction associated with higher ML/TF risk. Financial institutions should pay particular attention to those jurisdictions where corruption is perceived to be systemic or widespread.

3.3.6. The history of the business relationship with the respondent causes concern, for example because the number of transactions is not consistent with what the correspondent expects based on knowledge of the nature and size of the respondent.

3.3.7. The respondent fails to provide the information requested by the correspondent regarding CDD, EDD and the payer or beneficiary information.

3.4. The following factors can contribute to reducing the risk from the customer:

3.4.1. The respondent's PML/CTF controls are no less powerful than those required by international standards and applicable legislation;

3.4.2. The respondent is part of the same group as the correspondent, is not based in a jurisdiction associated with a higher ML/TF risk, and effectively complies with group PML standards that are no less stringent than those required from international standards and legislation in force.

3.5. The following factors may contribute to increased country or geographic risk:

3.5.1. The respondent is based in the jurisdiction associated with the highest ML/FT risk. Financial institutions should pay particular attention to jurisdictions which:

3.5.1.1. are identified as countries with a high risk of ML/TF

3.5.1.2. with a significant level of corruption and/or other related money laundering offences;

3.5.1.3. without adequate capacities of the legal and judicial system to effectively pursue criminal offenses;

3.5.1.4. without effective supervision of PML/CTF

3.5.1.5. with significant level of financing of terrorism or terrorist activities.

3.5.2. The Respondent conducts significant business with customers based in jurisdictions associated with higher ML/TF risk.

3.5.3. The respondent's parent headquarters is established in a jurisdiction associated with a higher ML/TF risk.

3.6. The following factors may contribute to the reduction of risk by country or geographical aspect:

3.6.1. the customer is from an EU country or a country that has established an effective system for the prevention of money laundering and terrorism financing, which is not subject to sanctions, embargoes or any similar measures;

4. All correspondents must perform CDD measures against the respondent, who is the correspondent's customer, on the basis of risk sensitivity. This means that correspondents must:

4.1. Identify and verify the identity of the respondent and its beneficial owner. As part of this, correspondents must obtain sufficient information about the respondent's business and reputation to establish that the money laundering risk associated with the respondent has not increased. In particular, correspondents must:

4.1.1. obtain information about the respondent's management and consider the significance, for financial crime prevention purposes, of any connection the respondent's management or ownership may have with PEPs or other high-risk individuals; and

4.1.2. consider, on a risk-sensitive basis, whether information is obtained about the respondent's core business, the types of customers it attracts, and the quality of its PML systems and controls (including publicly available information about any regulatory sanctions or criminal penalties of recent failures for PML) is appropriate. Where the respondent is a branch, subsidiary or associate, correspondents should also consider the status, reputation and PML controls of the parent company.

4.1.3. Create and document the nature and purpose of the service provided, as well as the responsibilities of each institution. This may include setting out, in writing, the scope, what products and services are offered, and how and by whom the correspondent banking facility can be used (e.g., whether it can be used by other banks through their relationships with respondent).

4.1.4. Monitor business relationships, including transactions, to identify changes in the respondent's risk profile and to identify unusual or suspicious behaviour, including activities that are inconsistent with the purpose of the services provided or that are contrary to commitments that have been made between the correspondent and the respondent. When the correspondent bank allows the respondent's customers direct access to accounts (e.g., accounts payable, or nested accounts), it must carry out continuous monitoring of the business relationship. Due to the nature of correspondent banks, post-execution monitoring is mandatory.

4.1.5. Ensure that the CDD information they hold is up to date.

Article 22

Trade Financing Instructions

1. Banks, during trade financing, must take into account the following risk factors and measures in addition to those defined by this Guideline:

1.1. The following factors may contribute in increasing the risk from transactions:

1.1.1. The transaction is unusually large given what is known about the customer's previous trading activity.

1.1.2. The transaction is highly structured, fragmented or complex, involving multiple parties, without any apparent legitimate rationale.

1.1.3. Copies of documents are used in situations where original documentation is needed, without reasonable explanations.

1.1.4. There are significant discrepancies in the documentation, for example between the description of the goods in the main documents (i.e., invoices and shipping documents) and the actual goods shipped, to the extent that this is apparent.

1.1.5. The type, quantity and value of the goods are inconsistent with the bank's knowledge of the buyer's business.

1.1.6. Bartered goods are of higher risk for money laundering purposes, for example some goods whose prices can fluctuate significantly, which can make prices difficult to be detected.

1.1.7. Bartered goods require an export license.

1.1.8. Commercial documentation does not comply with applicable laws or standards.

1.1.9. The unit price seems unusual, based on what the bank knows about goods and trade.

1.1.10. The transaction is otherwise unusual, for example the Letter of Credit Document is frequently changed without a clear rationale or the goods are sent through another jurisdiction for no apparent commercial reason.

1.2. The following factors may contribute in reducing the risk from transactions:

1.2.1. Independent inspection agents have verified the quality and quantity of goods.

1.2.2. Transactions involve parties who have established business relationships and who have a proven history of transacting with each other and due diligence has been performed on them previously.

1.3. The following factors may contribute to increased customer risk:

1.3.1. The transaction and/or parties involved are not consistent with what the bank knows about the customer's previous activity or line of business (e.g., the goods being

shipped, or shipping volumes, are not consistent with what is known about the business of the importer or exporter).

1.3.2. There are indications that the buyer and seller may be in cahoots, for example:

1.3.2.1. the buyer and the seller are controlled by the same person;

1.3.2.2. the businesses in the transactions have the same address, provide only one registered agent's address, or have other address discrepancies;

1.3.2.3. the buyer is willing and ready to accept or waive the discrepancies in the documentation.

1.3.3. The customer is unable or unwilling to provide the relevant documentation to support the transaction.

1.3.4. The buyer uses agents or third parties.

1.3.5. The following factors may contribute to reducing the risk:

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

1.3.7. The customer is listed on the stock exchange that meets the requirements for declarations similar to those of the EU.

1.4. The following factors can contribute to reducing the risk from the customer:

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

1.4.2. The customer is listed on the stock exchange that meets the requirements for declarations similar to those of the EU.

1.5. The following factors may contribute to increased country and geographic risk:

1.5.1. The country related to the transaction (including where the goods originate, for which they are destined, or have passed through the transaction, or where each party to the transaction is based) has currency exchange controls. This increases the risk that the true purpose of the transaction is to export currency in violation of local law.

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

1.6. The following factors may contribute to reducing country and geographic risk:

1.6.1. Trade takes place within the EU/European Economic Area.

1.6.2. Countries related to the transaction must have a PML regime/compliant with international standards and be associated with low levels of related criminal offences.

2. When a bank provides trade finance services to a customer, it must take steps, as part of its due diligence process, to understand the customer's business. Examples of the type of information the bank may receive include the countries the customer trades with, which trade routes are used, which goods are traded, with whom the customer does business (buyers, suppliers, etc.), whether the customer uses agents or third parties, and if so, where these agents or third parties are based. This helps banks understand who the customer is and help detect unusual or suspicious transactions.

Article 23

Instructions on electronic money issuers

1. Electronic money issuers must take into account the following risk factors and measures in addition to those defined by this Guideline:

   1.1. The following factors may contribute to increased risk from products, services and transactions:

      1.1.1. high value or unlimited value payments, loading and reloading, including cash unloading;

      1.1.2. high value payments, loading and reloading, including cash unloading;

      1.1.3. high or unlimited amounts of funds to be stored in the e-Money product/account

      1.1.4. funded by payments from unidentified third parties

      1.1.5. funded with other electronic money products

      1.1.6. allows person-to-person transfers;

      1.1.7. accepted as a payment method by a large number of merchants or points of sale;

      1.1.8. is specifically designed 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;

      1.1.9. can be used in cross-border transactions or in different jurisdictions;

      1.1.10. is designed to be used by persons other than customers, for example certain partner card products (but not low value gift cards);

      1.1.11. allows high value cash withdrawals.

   1.2. The following factors can contribute to reducing the risk of products, services and transactions:

      1.2.1. set low limits for payments, loading and reloading, including cash unloading (although financial institutions should note that a low limit alone may not be sufficient to reduce TF risk);

1.2.2. limits the number of payments, loading and reloading, including unloading of money in a certain period;

1.2.3. limits the amount of funds that can be stored in the e-money product/account at any time.

1.2.4. requires funds for purchase or loading to be verifiably unloaded from an account held in its own or joint customer's name at a bank or financial institution;

1.2.5. does not allow or strictly limits cash unloading;

1.2.6. can only be used within the country;

1.2.7. is accepted by a limited number of merchants or points of sale, whose business the electronic money issuer is familiar with;

1.2.8. is specifically designed to limit its use by merchants dealing in goods and services that are associated with a high risk of financial crime;

1.2.9. is accepted as a means of payment for limited types of low-risk services or products.

1.3. The following factors may contribute to increased customer risk:

1.3.1. The customer buys several electronic money products from the same issuer, often reloads the product or makes several unloads in a short period of time and without an economic justification;

1.3.2. Customer transactions are always below any value/transaction limit;

1.3.3. The product appears to be used by several persons whose identity is not known to the issuer (e.g., the product is used by several IP addresses at the same time);

1.3.4. There are frequent changes in customer identification data, such as home address or IP address, or linked bank accounts;

1.3.5. The product is not used for the purpose for which it was created.

1.4. The following factor can contribute to reducing the risk from the customer:

1.4.1. The product is available only to certain categories of customers, for example beneficiaries of social schemes or staff members of the company that issues them to cover corporate expenses.

1.5. The following factors may contribute to increased risk from distribution channels:

1.5.1.Distribution online and without physical presence, without adequate protection measures, such as electronic signatures, electronic identification documents that meet international field standards and measures against identity fraud.

1.5.2. Distribution through intermediaries who are not themselves reporting entities under the Law on PML/CTF, where applicable, when the electronic money issuer:

1.5.2.1. relies on the intermediary to fulfil some of the electronic money issuer's PML/CTF obligations; and

1.5.2.2. has not convinced itself that the intermediary has established adequate PML/CTF systems and controls.

1.5.2.3. unbundling of services, that is, the provision of electronic money services by several operationally independent service providers without proper supervision and coordination.

1.5.3. The institution, before signing a distribution agreement with a merchant, should understand the nature and purpose of the merchant's business to convince itself that the goods and services provided are legitimate and to assess the ML/TF risk associated with the merchant's business. In the case of a merchant that provides services online, financial institutions should also take steps to understand the type of customers this merchant attracts and determine the expected volume and size of transactions in order to spot suspicious or unusual transactions.

1.6. The following factors may contribute to increased country risk or geographic risk:

1.6.1. The payer is located in, or the product receives funds from sources in, a jurisdiction associated with higher ML/TF risk. Financial institutions should pay particular attention to jurisdictions known to provide funding or support for terrorist activities or where groups committing terrorist offenses are known to operate in those areas, and jurisdictions are subject to financial sanctions, embargoes or measures that relate to terrorism, terrorist financing or proliferation.

2. When the risk associated with a business relationship or occasional transaction has increased, the measures of EDD should be applied. These may include the following:

2.1. obtaining additional customer information during identification, such as the source of funds;

2.2. applying additional verification measures from a greater variety of reliable and independent sources (e.g., checking online databases) in order to verify the identity of the customer or beneficial owner;

2.3. obtaining additional information about the intended nature of the business relationship, for example by asking customers regarding their business or the jurisdictions to which they intend to transfer electronic money;

2.4. obtaining information about the merchant/payer, especially when the electronic money issuer has reason to suspect that its products are being used to purchase illegal or age-restricted goods;

2.5. applying controls on prevention of identity fraud to ensure that the customer is who they claim to be;

2.6. applying enhanced monitoring to customer relationships and individual transactions;

2.7. determining the source and/or destination of funds.

3. When the risk associated with a business relationship or occasional transaction is low, financial institutions may apply simplified due diligence measures. These may include the following:

3.1. verification of the customer's identity based on the payment withdrawn to the account in the customer's own or joint name or an account for which the customer can prove that there is supervision by a regulated bank or financial institution.

3.2. identity verification based on several sources;

3.3. identity verification based on less reliable sources;

3.4. using alternative methods to verify identity;

3.5. assuming the nature and intended purpose of the business relationship, where this is apparent, for example in the case of certain gift cards that do not fall under the closed circle/closed network exception;

Article 24

Instructions for money transfer institutions

1. Money transfer institutions should take into account the following risk factors and measures in addition to those defined by this Guideline:

1.1. The following factors may contribute to increased risk from products, services and transactions:

1.1.1. the product allows high value or unlimited value transactions;

1.1.2. the product or service is global in scope;

1.1.3. the transaction is based on cash or funded by anonymous electronic money;

1.1.4. transfers are made by one or more payers in different countries to a local beneficiary.

1.2. The following factors can contribute to reducing the risk of products, services and transactions:

1.2.1. the funds used during the transfer come from an account held in the payer's name at a local bank or financial institution.

1.3. The following factors may contribute to increased customer risk:

1.3.1. The customer owns or manages a business that deals with large cash flows.

1.3.2. The customer's business has a complex ownership structure

1.3.3. The customer's activity may be related to the financing of terrorism because the customer is publicly known to have extremist tendencies or is known to be associated with an organized crime group.

1.3.4. The customer's needs may be better served elsewhere, for example because the money transfer agency is not local to the customer or the customer's business.

1.3.5. The customer appears to be acting for someone else, for example the customer is being observed by other people or is seen outside the place where the transaction takes place, or the customer reads instructions from notes.

1.3.6. The customer's behaviour makes no apparent economic sense, for example, the customer accepts a poor exchange rate or high fees without asking, requires transactions in non-official currencies commonly used in the jurisdiction where the customer and/or recipient is located or requires or brings in large amounts of currencies that may depreciate or appreciate.

1.3.7. The customer's transactions are always below the applicable thresholds, including the CDD threshold for case transactions defined in applicable legislation.

1.3.8. Use of customer service is unusual, for example sending or receiving money from themselves to themselves or sending funds immediately after receiving them.

1.3.9. The customer appears to know very little or is unwilling to provide information about the transferor.

1.3.10. Some of the customers transfer funds to the same payee or appear to have the same identifying information, such as an address or phone number.

1.3.11. The incoming transaction is not accompanied by the required information on the sender or receiver.

1.3.12. The amount sent or received is inconsistent with the customer’s income (if known).

1.4. The following factors can contribute to reducing the risk from the customer:

1.4.1. The customer has been known for a long time, whose past behaviour has not raised suspicions and there are no indications that the risk of ML/TF may increase.

1.4.2. The amount transferred is low; however, financial institutions should note that low value alone is not sufficient to reduce TF risk.

1.5. The following factors may contribute to increased risk from service delivery channels:

1.5.1. There are no restrictions on the financing instrument, for example in the case of cash or payment by electronic money products, electronic transfer or cheques.

1.5.2. The distribution channel used provides a level of anonymity.

1.5.3. The Service is provided entirely online without appropriate safeguards.

1.5.4. The money remittance service is provided through agents who:

1.5.4.1. represent more than one leader;

1.5.4.2. have unusual turnover typologies compared to other agents in similar locations, for example unusually high or low numbers of transactions, unusually high cash transactions or a high number of transactions falling below the CDD threshold, or doing business outside normal business hours;

1.5.4.3. do a large part of their business with senders or receivers from jurisdictions associated with higher ML/FT risk;

1.5.4.4. appear to be uncertain about the implementation of PML/CTF policies within the group; or

1.5.4.5. are not from the financial sector and perform other business as their main business.

1.5.5. The remittance service is provided through an extremely complex payment chain, for example with a large number of intermediaries operating in different jurisdictions or allowing established (formal and informal) untraceable systems.

1.6. The following factors can contribute to reducing risk from service delivery channels:

1.6.1. Agents are regulated reporting entities themselves.

1.6.2. The service can only be funded by transfers from an account held in the customer's name at a bank or financial institution or an account over which the customer can demonstrate control.

1.7. The following factors may contribute to increased country risk or geographic risk:

1.7.1. The payer or payee is located, or the transaction is executed from an IP address, in a jurisdiction associated with a higher ML/TF risk. Financial institutions should pay particular attention to jurisdictions known to provide financing or support for terrorist activities or where groups that commit terrorist offenses are known to operate, and jurisdictions subject to financial sanctions, embargoes or measures related to terrorism, terrorist financing or weapons proliferation.

1.7.2. The payee is resident in a jurisdiction that has no formal banking sector or is less developed, which means informal money remittance services, such as *hawala*.

1.7.3. The counterparty of the institution is located in a third country associated with a higher ML/TF risk.

1.7.4. The payer or payee is located in a high-risk third country.

2. As money transfer institutions' business is largely transaction-based, consideration should be given to what monitoring and control systems they put in place to ensure that they detect money

laundering and terrorist financing attempts even when information about the CDD that they hold on the customer is basic or absent because no business relationship has been established.

3. Money transfer institutions, in any case, must decide the following:

   3.1. systems to identify related transactions;

   3.2. systems to identify whether transactions from different customers are intended for the same beneficiary;

   3.3. systems to allow as much as possible the creation of the source of funds and the destination of funds;

   3.4. systems that allow full traceability of both transactions and the number of operators involved in the payment chain; and

   3.5. systems to ensure that throughout the payment chain only those officially authorized to provide remittance services can intervene.

4. When the risk associated with occasional transactions or business relationships is increased, money transfer institutions should apply enhanced due diligence measures, including, where appropriate, increased monitoring of transactions (e.g., increased frequency or lower thresholds). Conversely, when the risk associated with the occasional transaction or business relationship is low, money transfer institutions may apply simplified due diligence measures consistent with the measures set out in this Guideline.

5. Money transfer institutions that use agents to provide services must know who their agents are. As part of this, money transfer institutions must establish and maintain appropriate and risk-based policies and procedures to combat the risk that their agents may engage in, or be used for, ML/TF, including the following:

   5.1. Identification of the person who owns or controls the agent, when the agent is a legal entity, to make sure that the risk of ML/TF, to which the money transfer institution is exposed, as a result of the use of this agent, has not increased.

   5.2. Obtaining documents that the directors and other persons responsible for the administration of the agent are fit and proper persons, including considering the criteria for fit and proper, integrity and reputation. Any verification that the money transfer institution does must be proportionate to the nature, complexity and level of ML/TF risk inherent in the remittance services provided by the agent and may be based on the money transfer institution's CDD procedures.

   5.3. Taking reasonable steps to convince oneself that the agent's internal controls for PML/CTF are adequate and remain adequate throughout the relationship, for example by monitoring a sample of the agent's transactions or reviewing the agent's on-site controls. Where the internal controls of PML/CTF agents differ from those of the transfer institution, for example because the agent represents more than the money transfer institution or because the agent is itself a reporting entity under applicable PML/CTF legislation, the money

transfer institution must assess and manage the risk that these changes may affect it, and the agent's compliance with PML/CTF.

5.4. Providing PML/CTF training to agents to ensure that they have an adequate understanding of the relevant PML/CTF risks and the quality of PML/CTF controls that the money transfer institution expects to have.

Article 25

Instructions on insurance companies

1. Insurers should consider the following risk factors and measures in addition to those set out in this Guideline:

1.1. The following factors may contribute to increased risk from products, services and transactions:

1.1.1. Payment flexibility that the product allows, for example:

1.1.1.1. payments from unidentified third parties;

1.1.1.2. high value or unlimited value premium payments, overpayments or large volumes of lower value premiums;

1.1.1.3. cash payment

1.1.2. Ease of access to accumulated funds, for example the product allows partial withdrawal or early delivery at any time, with limited fees or commissions.

1.1.3. Negotiability, for example the product can:

1.1.3.1. be sold on a secondary market;

1.1.3.2. be used as collateral for a loan.

1.1.4.Anonymity, for example the product allows or facilitates customer anonymity.

1.2. The following factors can contribute to reducing the risk of products, services and transactions:

1.2.1. there is no investment element;

1.2.2. no payment facilities to third parties;

1.2.3. requires that the total investment be reduced by a low value;

1.2.4. it is a life insurance policy where the premium is low;

1.2.5. allows only regular premium payments of small amounts, for example without overpayments;

1.2.6. is only accessible through employers, for example a pension, pension contribution or similar scheme providing retirement benefits to employees, where contributions are made through deduction from wages and the scheme rules do not allow a member's interest to be assigned under the scheme;

1.2.7. cannot be recovered in the short or medium term, as in the case of pension schemes without the possibility of early surrender;

1.2.8. cannot be used as collateral;

1.2.9. does not allow cash payments;

1.2.10. there are conditions that must be met to benefit from the tax benefits.

1.3. The following factors may contribute to increased risk from the customer and beneficiaries:

1.3.1. legal entities whose structure makes it difficult to identify the beneficial owner;

1.3.2. the customer or the beneficial owner of the customer is a PEP;

1.3.3. the beneficiary of the policy or the beneficial owner of such beneficiary is a PEP;

1.3.4. the customer's age is unusual for the type of product requested (e.g., the customer is too young or too old);

1.3.5. the contract does not match the state of the customer’s property;

1.3.6. the customer’s profession or activities are considered to be particularly predisposed to money laundering, for example because it is known to involve a large circulation of cash or exposed to a high risk of corruption;

1.3.7. the contract is registered by a "money custodian", such as a trust company, acting on behalf of the customer;

1.3.8. the policyholder and/or contract beneficiary are companies with nominee shareholders and/or bearer shares.

1.3.9. the customer often transfers the contract to another insurer;

1.3.10. frequent and unexplained cancellations, especially when the refund is made to different bank accounts;

1.3.11. the customer makes frequent or unexpected use of the "free lock"/"cooling off" period provisions, especially when the refund is made to an apparently unrelated third party;[1]

1.3.12. the customer incurs high costs by requiring early termination of a product;

[1]A 'free lock' provision is a contractual provision, often mandatory under local law, which allows a policy owner or annuitant of a life insurance or annuity contract to review a contract for a specified number of days and return it for a full refund.

1.3.13. the customer transfers the contract to an apparently unrelated third party;

1.3.14. the customer’s request to change or increase the insured amount and/or the premium payment is unusual or high;

1.3.15. the insurer is notified of a change in beneficiary only when a request is made;

1.3.16. the customer amends the beneficiary clause and names a third party that is apparently unrelated;

1.3.17. the insurer, the customer, the beneficial owner, the beneficiary or the beneficial owner of the beneficiary are in different jurisdictions.

1.3.18. the consumer uses unusual payment methods, such as structured funds or other forms of payment instruments that promote anonymity;

1.3.19. payments from different bank accounts without clarification;

1.3.20. payments from banks that are not located in the customer's place of residence;

1.3.21. the customer makes frequent payments or in high amounts, when this was not expected;

1.3.22. payments received from unrelated third parties;

1.3.23. added contribution to a pension plan close to the date of retirement.

1.4. The following factors can contribute to the reduction of risk in the case of life insurance purchased by corporations, when the customer is:

1.4.1. a bank or financial institution that is subject to anti-money laundering and anti-terrorist financing requirements and is supervised for compliance with these requirements;

1.4.2. a public company listed on a stock exchange and subject to regulatory disclosure requirements (either by stock exchange rules, or by law or by applicable means) that impose requirements to ensure adequate transparency of beneficial ownership, or a majority subsidiary of such a company;

1.4.3. a public administration or public enterprise.

1.5. The following factors may contribute to increased risk from service delivery channels:

1.5.1. Sales without a physical presence, such as sales online, by mail or telephone, without adequate safeguards, such as electronic signatures or electronic identification documents defined by international standards.

1.5.2. long chain of intermediaries;

1.5.3. intermediary is used in unusual circumstances (e.g., unexplained geographical distances).

1.6. The following factors can contribute to reducing risk from service delivery channels:

1.6.1. Intermediaries are known to the insurer, which is convinced that the intermediary implements CDD measures in proportion to the risk associated with the relationship and in accordance with those required by applicable legislation.

1.6.2. 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.

1.7. The following factors may contribute to increased country or geographic risk:

1.7.1. The insurer, the customer, the beneficial owner, the beneficial owner's beneficiary is established in or has links to jurisdictions with a higher ML/TF risk. Insurers should pay particular attention to jurisdictions without effective PML/CTF oversight.

1.7.2. Premiums are paid through accounts held at financial institutions established in jurisdictions associated with higher ML/TF risk. Insurers should pay particular attention to jurisdictions without effective PML/CTF oversight.

1.7.3. The intermediary is established in or has ties to related jurisdictions with a higher ML/TF risk. Insurers should pay particular attention to jurisdictions without effective PML/CTF oversight.

1.8. The following factors can contribute to reducing country or geographic risk:

1.8.1. The country is identified by reliable sources, such as mutual evaluations or detailed evaluation reports, as a country with an effective PML/CTF system.

1.8.2. The country is identified by reliable sources as having a low level of corruption and other criminal activity.

2. Insurers must apply due diligence measures, not only to the customer and the beneficial owner, but also to the beneficiaries, immediately after they are identified or designated. This means that the entity must:

2.1. obtain the name of the beneficiary when a natural or legal person or an agreement has been identified as the beneficiary; or

2.2. obtain sufficient information to be convinced that the identity of the beneficiaries can be determined at the time of payment where the beneficiaries are a class of persons or defined by certain characteristics. For example, when the beneficiary is his "future grandchildren," the insurer may obtain information about policyholder’s children.

3. The reporting entity must verify the identity of the beneficiaries at the latest at the time of payment.

4. When the reporting entity knows that the life insurance is assigned to a third party that receives the policy value, they must identify the beneficial owner at the time of assignment.

5. In high-risk situations, the following additional due diligence measures may be appropriate:

5.1. When the customer uses the "free lock"/"cooling-off" period, the premium must be returned to the customer's bank account from which the funds were paid. Insurers should ensure that they have verified the identity of the customer before making a refund, especially where the premium is large or the circumstances arising are unusual. Insurers should also consider whether the cancellation raises suspicions about the transaction and whether filing a suspicious activity report is appropriate.

5.2. Additional steps may be taken to strengthen the entity's knowledge of the customer, beneficial owner, beneficiary or beneficial owner of the beneficiary, payers and third party's payers. Examples include the following:

5.2.1. verifying the identity of other relevant parties, including payers and third party third parties, before starting the business relationship;

5.2.2. obtaining additional information to determine the intended nature of the business relationship;

5.2.3. obtaining additional customer information and more regularly updating customer and beneficial owner identification data;

5.2.4. if the payer is different from the customer, the reason behind this must be determined;

5.2.5. identity verification based on more than one reliable and independent source;

5.2.6. determining the source of the customer's assets and funds, for example employment and salary details, inheritance or divorce arrangements;

5.2.7. where possible, the beneficiary should be identified at the start of the business relationship, rather than waiting until they are identified or determined, given that the beneficiary may change during the life of the policy;

5.2.8. identifying and verifying the identity of the beneficial owner of the beneficiary;

5.2.9. steps must be taken to determine whether the customer is a PEP and reasonable steps must be taken to determine whether the beneficiary or the beneficial owner of the beneficiary is a PEP at the time of assignment, in whole or in part, of the policy or, the latest, at the time of payment;

5.2.10. the first payment must be made through an account in the customer's name with a bank.

5.3. When the risk associated with a PEP relationship is high, insurers should not only implement measures for CDD, but also inform senior management before the policy is paid out so that senior management can have a clear picture of the risk of PML/CTF related to the situation and decide on the most appropriate measures to mitigate that risk; in addition, the entity must perform EDD throughout the entire business relationship. More

frequent and more detailed monitoring of transactions (including where necessary, tracing the source of funds) may be required.

6. In low-risk situations, the following simplified due diligence measures may be appropriate:

6.1. The entity may be able to assume that verification of the customer's identity has been performed based on a payment made to the account in the customer's name with a bank.

6.2. The entity may assume that the verification of the identity of the beneficiary of the contract is carried out on the basis of a payment made to an account in the name of the beneficiary at a regulated financial institution.

Article 26

Instructions on foreign currency exchange offices

1. Foreign currency exchange offices should take into account the following risk factors and measures in addition to those defined by this Guideline:

1.1. The following factors may contribute to increased risk from products, services and transactions:

1.1.1. The transaction is extremely large in absolute terms or compared to the customer's economic profile;

1.1.2. The transaction has no apparent economic or financial purpose;

1.2. The following factors can contribute to reducing the risk of products, services and transactions:

1.2.1. The amount exchanged is low, however it should be noted that low amounts alone are not sufficient to reduce the risk of terrorist financing.

1.3. The following factors may contribute to increased customer risk:

1.3.1. the customer's transactions are slightly below the applicable limit for the application of due diligence measures, especially when they are frequent or within a short period of time;

1.3.2. the customer cannot or does not provide information about the origin of the funds;

1.3.3. the customer wants to exchange large amounts of foreign currency which is not convertible or is not frequently used;

1.3.4. the customer exchanges large amounts of low-denomination banknotes for higher-denomination banknotes in another currency; or vice versa.

1.3.5. Customer behaviour makes no apparent economic sense;

1.3.6. The customer visits several premises of the same currency exchange office on the same day (to the extent known by the currency exchange office);

1.3.7. The customer asks questions about the identification threshold and/or refuses to answer random or routine questions;

1.3.8. The customer converts funds of one foreign currency into another foreign currency;

1.3.9. Exchange of large amounts or frequent exchanges unrelated to the customer's business;

1.3.10. The currency sold by the customer does not correspond to his or her country of citizenship or residence;

1.3.11. The customer buys currency from an unusual country compared to his/her location without any logical explanation;

1.3.12. The customer purchases currency that does not match what is known about the customer's country of destination;

1.3.13. The customer buys or sells a large amount of a currency from a jurisdiction associated with significant levels of major ML offenses or terrorist activity;

1.3.14. The customer’s business is associated with a higher ML/TF risk, for example casinos, buying/selling of precious metals and gems.

1.4. The following factors may contribute to the increased risk of providing services:

1.4.1. The service is provided entirely online without adequate safeguards;

1.4.2. The provision of services is carried out through a network of agents.

1.5. The following factors may contribute to increased country and geographic risk:

1.5.1. The business of the currency exchange office is located in a jurisdiction associated with higher ML/TF risk;

2. Foreign currency exchange offices should clearly define in their internal policies and procedures at what point they should perform due diligence on their casual customers. This should include the following:

2.1. The situation when a transaction or related identified transactions reach 10,000 euros. Policies and procedures should clearly define at what point a series of one-off transactions constitutes a business relationship, taking into account the context of the firms' activities (i.e., the normal average size of a one-off transaction from their normal customers).

2.2. Situations where there are suspicions of money laundering or terrorist financing.

3. Foreign currency exchange offices must also establish systems and controls for the following:

3.1. identifying related transactions (for example, to find out if the same customer goes to multiple offices within a short period of time); monitoring transactions in a manner that is appropriate and effective in proportion to the size of the office, the number of its offices, the size and volume of transactions;

3.2. the type of activities performed, its delivery channels and the risks identified in the business-wide risk assessment.

4. In situations where the risk of ML/TF is high, currency exchange offices should apply enhanced due diligence measures in accordance with this Guideline, including, where necessary, increased monitoring of transactions as well as obtaining more information relating to the nature and purpose of the business, or the source of the customer's funds.

5. In situations where the ML/TF risk is low, currency exchange offices may consider implementing simplified due diligence measures such as the following:

5.1. postponing the verification of the customer's identity to a certain later date after the establishment of the relationship.

5.2. verifying the customer's identity based on a payment withdrawn to an account in the customer's sole or joint name at a banking institution.

Article 27
Transitional provisions

Financial institutions must prepare until 1 February 2024 for the applicability of the provisions of this Guideline.

Article 28
Entry into force

This Guideline shall enter into force on the day of its approval.

Ahmet Ismaili
Chairman of the Executive Board