EBA/GL/2021/02 (consolidated version)

1 March 2021

➢O

Guidelines

under Articles 17 and 18(4) of Directive (EU) 2015/849 on customer due diligence and the factors credit and financial institutions should consider when assessing the money laundering and terrorist financing risk associated with individual business relationships and occasional transactions ("The ML/TF Risk Factors Guidelines"), repealing and replacing Guidelines JC/2017/37

		Application date
➢O		07.10.2021
Amended by:		
➢A1	EBA/GL/2023/03	03.10.2023
	EBA/GL/2021/02 (consolidated version)	07.10.2021

1. Compliance and reporting obligations

Status of these guidelines

1. This document contains Guidelines issued pursuant to Article 16 of Regulation (EU) No 1093/2010[1]. In accordance with Article 16(3) of Regulation (EU) No 1093/2010, competent authorities and financial institutions must make every effort to comply with the Guidelines.

2. Guidelines set out the EBA's view of appropriate supervisory practices within the European System of Financial Supervision or of how Union law should be applied in a particular area. Competent authorities as defined in Article 4(2) of Regulation (EU) No 1093/2010 to whom Guidelines apply should comply by incorporating them into their practices as appropriate (e.g. by amending their legal framework or their supervisory processes), including where Guidelines are directed primarily at institutions.

Reporting requirements

3. According to Article 16(3) of Regulation (EU) No 1093/2010, competent authorities must notify the EBA that they comply or intend to comply with these Guidelines, or otherwise give reasons for non-compliance, by 07.09.2021. In the absence of any notification by this deadline, competent authorities will be considered by the EBA to be non-compliant. Notifications should be sent by submitting the form available on the EBA website to compliance@eba.europa.eu with the reference 'EBA/GL/2021/02'. Notifications should be submitted by persons with appropriate authority to report compliance on behalf of their competent authorities. Any change in the status of compliance must also be reported to the EBA.

4. Notifications will be published on the EBA website, in line with Article 16(3).

[1] Regulation (EU) No 1093/2010 of the European Parliament and of the Council of 24 November 2010 establishing a European Supervisory Authority (European Banking Authority), amending Decision No 716/2009/EC and repealing Commission Decision 2009/78/EC, (OJ L 331, 15.12.2010, p.12).

2. Subject matter, scope and definitions

Subject matter

5. These guidelines set out factors firms should consider when assessing the money laundering and terrorist financing (ML/TF) risk associated with their business, and with a business relationship or an occasional transaction with any natural or legal person ('the customer'). They also set out how firms should adjust the extent of their customer due diligence (CDD) measures in a way that is commensurate to the ML/TF risk they have identified.

6. These guidelines' main focus is on risk assessments of individual business relationships and occasional transactions, but firms should use these guidelines *mutatis mutandis* when assessing ML/TF risk across their business in line with Article 8 of Directive (EU) 2015/849.

7. The factors and measures described in these guidelines are not exhaustive and firms should consider other factors and measures as appropriate.

Scope of application

8. These guidelines are addressed to credit and financial institutions as defined in Article 3(1) and 3(2) of Directive (EU) 2015/849 and competent authorities responsible for supervising these firms' compliance with their anti-money laundering and counter-terrorist financing (AML/CFT) obligations.

9. Competent authorities should use these guidelines when assessing the adequacy of firms' risk assessments and AML/CFT policies and procedures.

10. Competent authorities should also consider the extent to which these guidelines can inform the assessment of the ML/TF risk associated with their sector, which forms part of the risk-based approach to supervision. The ESAs have issued guidelines on risk-based supervision in accordance with Article 48(10) of Directive (EU) 2015/849.

11. Compliance with the European financial sanctions regime is outside the scope of these guidelines.

Definitions

12. For the purpose of these guidelines, the following definitions shall apply:

    a) 'Competent authorities' means the authorities competent for ensuring firms' compliance with the requirements of Directive (EU) 2015/849 as transposed by national

legislation[2].

b) 'Firms' means credit and financial institutions as defined in Article 3(1) and (2) of Directive (EU) 2015/849.

c) 'Inherent risk' means the level of risk before mitigation.

d) 'Jurisdictions associated with higher ML/TF risk' means countries that, based on an assessment of the risk factors set out in Title I of these guidelines, present a higher ML/TF risk. This excludes 'high-risk third countries' identified as having strategic deficiencies in their AML/CFT regime, which pose a significant threat to the Union's financial system (Article 9 of Directive (EU) 2015/849).

e) 'Non-face to face relationships or transactions' means any transaction or relationship where the customer is not physically present, that is, in the same physical location as the firm or a person acting on the firm's behalf. This includes situations where the customer's identity is being verified via video-link or similar technological means.

A1

f) 'Not-for-profit organisation' is a legal person or arrangement or an organisation that primarily engages in raising or disbursing funds for purposes such as charitable, religious, cultural, educational, social or fraternal purposes.

O

g) 'Occasional transaction' means a transaction that is not carried out as part of a business relationship as defined in Article 3(13) of Directive (EU) 2015/849.

h) 'Pooled account' means a bank account opened by a customer, for example a legal practitioner or notary, for holding their clients' money. The clients' money will be commingled, but clients will not be able directly to instruct the bank to carry out transactions.

i) 'Residual risk' means the level of risk that remains after mitigation.

j) 'Risk' means the impact and likelihood of ML/TF taking place.

k) 'Risk appetite' means the level of risk a firm is prepared to accept.

l) 'Risk factors' means variables that, either on their own or in combination, may increase or decrease the ML/TF risk posed by an individual business relationship or occasional transaction.

m) 'Risk-based approach' means an approach whereby competent authorities and firms identify, assess and understand the ML/TF risks to which firms are exposed and take AML/CFT measures that are proportionate to those risks.

n) 'Shell bank' as defined in point (17) of Article 3 of Directive (EU) 2015/849.

o) 'Source of funds' means the origin of the funds involved in a business relationship or

[2] Article 4(2)(ii), Regulation (EU) No 1093/2010; Article 4(2)(ii), Regulation (EU) No 1094/2010; Article 4(3)(ii), Regulation (EU) No 1093/2010

occasional transaction. It includes both the activity that generated the funds used in the business relationship, for example the customer's salary, as well as the means through which the customer's funds were transferred.

p) 'Source of wealth' means the origin of the customer's total wealth, for example inheritance or savings.

3. Implementation

Date of application

1. These Guidelines will apply three months after publication in all EU official languages.

Title I: General Guidelines

These guidelines come in two parts. Title I is general and applies to all firms. Title II is sector-specific. Title II is incomplete on its own and should be read in conjunction with Title I.

Guideline 1: Risk assessments: key principles for all firms

1.1. Firms should ensure that they have a thorough understanding of the ML/TF risks to which they are exposed.

General considerations

1.2. To comply with their obligations set out in Directive (EU) 2015/849, firms should assess:

a) the ML/TF risk to which they are exposed as a result of the nature and complexity of their business (the business-wide risk assessment); and

b) the ML/TF risk to which they are exposed as a result of entering into a business relationship or carrying out an occasional transaction (individual risk assessments).

Each risk assessment should consist of two distinct but related steps:

a) the identification of ML/TF risk factors; and

b) the assessment of ML/TF risk.

1.3. When assessing the overall level of residual ML/TF risk associated with their business and with individual business relationships or occasional transactions, firms should consider both, the level of inherent risk, and the quality of controls and other risk mitigating factors.

1.4. As set out in Article 8(2) of Directive (EU) 2015/849, firms should record and document their business-wide risk assessment, as well as any changes made to this risk assessment in a way that makes it possible for the firm, and for competent authorities, to understand how it was conducted, and why it was conducted in a particular way.

1.5. Firms that are credit institutions and investment firms should also refer to the EBA's internal governance guidelines in this context.[3]

[3] Guidelines on internal governance, EBA/GL/2017/11

Keeping risk assessments up to date

1.6. Firms should put in place systems and controls to keep their assessments of the ML/TF risk associated with their business, and with their individual business relationships under review to ensure that their assessment of ML/TF risk remains up to date and relevant.

1.7. The systems and controls that firms should put in place to ensure their individual and business-wide risk assessments remain up to date should include:

a) Setting a date for each calendar year on which the next business-wide risk assessment update will take place, and setting a date on a risk sensitive basis for the individual risk assessment to ensure new or emerging risks are included.

b) Where the firm becomes aware before that date that a new ML/TF risk has emerged, or an existing one has increased, this should be reflected in their individual and business-wide risk assessments as soon as possible; and

c) Carefully recording issues throughout the relevant period that could have a bearing on risk assessments, such as internal suspicious transaction reports, compliance failures and intelligence from front office staff.

1.8. As part of this, firms should ensure that they have systems and controls in place to identify emerging ML/TF risks and that they can assess these risks and, where appropriate, incorporate them into their business-wide and individual risk assessments in a timely manner.

1.9. The systems and controls that firms should put in place to identify emerging risks should include:

a) Processes to ensure that internal information, such as information obtained as part of a firm's ongoing monitoring of business relationships, is reviewed regularly to identify trends and emerging issues in relation to both, individual business relationships and the firm's business.

b) Processes to ensure that the firm regularly reviews relevant information sources, including those specified in guidelines 1.28 to 1.30 , and in particular:

i. In respect of individual risk assessments,

a. terror alerts and financial sanctions regimes, or changes thereto, as soon as they are issued or communicated and ensure that these are acted upon as necessary; and

b. media reports that are relevant to the sectors or jurisdictions in which the firm is active.

ii. In respect of business-wide risk assessments,

a. law enforcement alerts and reports;

b. thematic reviews and similar publications issued by competent authorities; and

c. Processes to capture and review information on risks, in particular risks relating to new categories of customers, countries or geographical areas, new products, new services, new distribution channels and new compliance systems and controls.

c) Engagement with other industry representatives and competent authorities (e.g. round tables, conferences and training), and processes to feed back any findings to relevant staff.

1.10. Firms should determine the frequency of wholesale reviews of their business-wide and individual risk assessments methodology on a risk-sensitive basis.

Business-wide risk assessments

1.11. Business-wide risk assessments should help firms understand where they are exposed to ML/TF risk and which areas of their business they should prioritise in the fight against ML/TF.

1.12. To this end, firms should take a holistic view of the ML/TF risks to which they are exposed, by identifying and assessing the ML/TF risk associated with the products and services they offer, the jurisdictions they operate in, the customers they attract and the transaction or delivery channels they use to service their customers..

1.13. Firms should:

a) Identify risk factors based on information from a variety of internal and external sources, including the sources listed in Guidelines 1.30 to 1.31;

b) have regard to relevant risk factors in Titles I and II of these Guidelines; and

c) take into account wider, contextual, factors such as sectoral risk and geographical risk, that could have a bearing on their ML/TF risk profiles.

1.14. Firms should ensure that their business-wide risk assessment is tailored to their business profile and takes into account the factors and risks specific to the firm's business, whether the firm draws up its own business-wide risk assessment or contracts an external party to draw up its business-wide risk assessment. Similarly, where a firm is part of a group that draws up a group-wide risk assessment, the firm should consider whether the group-wide risk assessment is sufficiently granular and specific to reflect the firm's business and the risks

to which it is exposed as a result of the group's links to countries and geographical areas, and complement the group-wide risk assessment if necessary. If the group is headquartered in a country associated with a high level of corruption, the firm should reflect this in its risk assessment even if the group-wide risk assessment stays silent on this point.

1.15. A generic ML/TF risk assessment that has not been adapted to the specific needs and business model of the firm ('an off-the-shelf ML/TF risk assessment'), or a group-wide risk assessment that is applied unquestioningly, is unlikely to meet the requirements in Article 8 of Directive (EU) 2015/849.

Proportionality

1.16. As set out in Article 8 of Directive (EU) 2015, 849, the steps a firm takes to identify and assess ML/TF risk across its business must be proportionate to the nature and size of each firm. Small firms that do not offer complex products or services and that have limited or purely domestic exposure, may not need a complex or sophisticated risk assessment.

Implementation

1.17. Firms should

a) make their business-wide risk assessment available to competent authorities ;

b) Take steps to ensure that staff understand the business-wide risk assessment, and how it affects their daily work in line with Article 46 (1) of Directive (EU) 2015/849; and

c) inform senior management about the results of their business-wide risk assessment, and ensure that senior management is provided with sufficient information to understand, and take a view on, the risk to which their business is exposed.

Linking the business-wide and individual risk assessments

1.18. Firms should use the findings from their business-wide risk assessment to inform their AML/CFT policies, controls and procedures, as set out in Article 8(3) and (4) of Directive (EU) 2015/849. Firms should ensure that their business-wide risk assessment also reflects the steps taken to assess the ML/TF risk associated with individual business relationships or occasional transactions and their ML/TF risk appetite.

1.19. To comply with Guideline 1.18, and also having regard to Guidelines 1.21 and 1.22, firms should use the business-wide risk assessment to inform the level of initial customer due diligence that they will apply in specific situations, and to particular types of customers, products, services and delivery channels.

1.20. Individual risk assessments should inform, but are no substitute for, a business-wide risk assessment.

Individual risk assessments

1.21. Firms should find out which ML/TF risks they are, or would be, exposed to as a result of entering into, or maintaining, a business relationship or carrying out an occasional transaction.

1.22. When identifying ML/TF risks associated with a business relationship or occasional transaction, firms should consider relevant risk factors including who their customer is, the countries or geographical areas they operate in, the particular products, services and transactions the customer requires and the channels the firm uses to deliver these products, services and transactions.

Initial Customer Due Diligence

1.23. Before entering into a business relationship or carrying out an occasional transaction, firms should apply initial CDD in line with Article 13(1)(a), (b) and (c) and Article 14(4) of Directive (EU) 2015/849.

1.24. Initial CDD should include at least risk-sensitive measures to:

a) identify the customer and, where applicable, the customer's beneficial owner;

b) verify the customer's identity on the basis of reliable and independent sources and,where applicable, verify the beneficial owner's identity in such a way that the firm is satisfied that it knows who the beneficial owner is; and

c) establish the purpose and intended nature of the business relationship.

1.25. Firms should adjust the extent of initial CDD measures on a risk-sensitive basis, taking into account the findings from their business-wide risk assessment. Where the risk associated with a business relationship is likely to be low, and to the extent permitted by national legislation, firms may be able to apply simplified customer due diligence measures (SDD). Where the risk associated with a business relationship is likely to be increased, firms must apply enhanced customer due diligence measures (EDD).

Obtaining a holistic view

1.26. Firms should gather sufficient information so that they are satisfied that they have identified all relevant risk factors at the beginning of the business relationship and throughout the business relationship or before carrying out the occasional transaction. Where necessary, firms should apply additional CDD measures, and assess those risk factors to obtain a holistic view of the risk associated with a particular business relationship or occasional transaction.

1.27. There is no expectation that firms should draw up a complete customer risk profile for occasional transactions.

Ongoing customer due diligence

1.28. Firms should use information obtained during the course of the business relationship for individual risk assessment purposes (see 'Monitoring' in Guideline 4).

Sources of information

1.29. To identify ML/TF risk, firms should refer to information from a variety of sources, which can be accessed individually or through commercially available tools or databases that pool information from several sources.

1.30. Firms should always consider the following sources of information:

a) the European Commission's supranational risk assessment;

b) the European Commission's list of high-risk third countries;

c) information from governments, such as governments' national risk assessments, policy statements and alerts, and explanatory memorandums to relevant legislation;

d) information from regulators, such as guidance and the reasoning set out in regulatory fines;

e) information from Financial Intelligence Units (FIUs) and law enforcement agencies, such as threat reports, alerts and typologies; and

f) information obtained as part of the initial CDD process and ongoing monitoring.

1.31. Other sources of information firms should consider include, but are not limited to:

a) the firm's own knowledge and professional expertise;

b) information from industry bodies, such as typologies and emerging risks;

c) information from civil society, such as corruption indices and country reports;

d) information from international standard-setting bodies such as mutual evaluation reports or legally non-binding blacklists, including those listed in guidelines 2.11 to 2.15 ;

e) information from credible and reliable open sources, such as reports in reputable newspapers;

f) information from credible and reliable commercial organisations, such as risk and intelligence reports; and

g) information from statistical organisations and academia.

1.32. Firms should determine the type and numbers of sources on a risk-sensitive basis, taking into account the nature and complexity of their business. Firms should not normally rely on only one source to identify ML/TF risks.

Guideline 2: Identifying ML/TF risk factors

2.1. Firms should identify risk factors relating to their customers, countries or geographical areas, products and services, and delivery channels in the wayset out in these Guidelines, having also regard to the non-exhaustive list of factors set out in Annexes II and III of Directive (EU) 2015/849.

2.2. Firms should note that the following risk factors are not exhaustive, nor is there an expectation that firms will consider all risk factors in all cases.

Customer risk factors

2.3. When identifying the risk associated with their customers, including their customers' beneficial owners, firms should consider the risk related to:

a) the customer's and the customer's beneficial owner's business or professional activity;

b) the customer's and the customer's beneficial owner's reputation; and

c) the customer's and the customer's beneficial owner's nature and behaviour, including whether this could point to increased TF risk.

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

a) Does the customer or beneficial owner have links to sectors that are commonly associated with higher corruption risk, such as construction, pharmaceuticals and healthcare, the arms trade and defence, the extractive industries or public procurement?

b) Does the customer or beneficial owner have links to sectors that are associated with higher ML/TF risk, for example certain Money Service Businesses, casinos or dealers in precious metals?

c) Does the customer or beneficial owner have links to sectors that involve significant amounts of cash?

d) Where the customer is a legal person, trust, or other type of legal arrangement, what is the purpose of their establishment? For example, what is the nature of their business?

e) Does the customer have political connections, for example, are they a Politically Exposed Person (PEP), or is their beneficial owner a PEP? Does the customer or beneficial owner have any other relevant links to a PEP, for example are any of the customer's directors PEPs and, if so, do these PEPs exercise significant control over the customer or beneficial owner? Where a customer or their beneficial owner is a PEP, firms must always apply EDD measures in line with Article 20 of Directive (EU) 2015/849.

f) Does the customer or beneficial owner hold another prominent position or enjoy a high public profile that might enable them to abuse this position for private gain? For example, are they senior local or regional public officials with the ability to influence the awarding of public contracts, decision-making members of high-profile sporting bodies or individuals who are known to influence the government and other senior decision-makers?

g) Is the customer a legal person subject to enforceable disclosure 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 for listing?

h) Is the customer a credit or financial institution acting on its own account from a jurisdiction with an effective AML/CFT regime and is it supervised for compliance with local AML/CFT obligations? Is there evidence that the customer has been subject to supervisory sanctions or enforcement for failure to comply with AML/CFT obligations or wider conduct requirements in recent years?

i) Is the customer a public administration or enterprise from a jurisdiction with low levels of corruption?

j) Is the customer's or the beneficial owner's background consistent with what the firm knows about their former, current or planned business activity, their business's turnover, the source of funds and the customer's or beneficial owner's source of wealth?

2.5. The following risk factors may be relevant when identifying the risk associated with a customer's or beneficial owners' reputation:

a) Are there adverse 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 the beneficial owner? If so, are these reliable and credible? Firms should determine the credibility of allegations on the basis of the quality and independence of the source of the data and the persistence of reporting of these allegations, among other considerations. Firms should note that the absence of criminal convictions alone may not be sufficient to dismiss allegations of wrongdoing.

b) Has the customer, beneficial owner or anyone publicly known to be closely associated with them had their assets frozen due to administrative or criminal proceedings or allegations of terrorism or terrorist financing? Does the firm have reasonable grounds to suspect that the customer or beneficial owner or anyone publicly known to be closely associated with them has, at some point in the past, been subject to such an asset freeze?

c) Does the firm know if the customer or beneficial owner has been the subject of a suspicious transactions report in the past?

d) Does the firm have any in-house information about the customer's or the beneficial owner's integrity, obtained, for example, in the course of a long-standing business relationship?

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

a) Does the customer have legitimate reasons for being unable to provide robust evidence of their identity, perhaps because they are an asylum seeker?

b) Does the firm have any doubts about the veracity or accuracy of the customer's or beneficial owner's identity?

c) Are there indications that the customer might seek to avoid the establishment of a business relationship? For example, does the customer look to carry out one transaction or several one-off transactions where the establishment of a business relationship might make more economic sense?

d) Is the customer's ownership and control structure transparent and does it make sense? If the customer's ownership and control structure is complex or opaque, is there an obvious commercial or lawful rationale?

e) Does the customer issue bearer shares or does it have nominee shareholders?

f) Is the customer a legal person or arrangement that could be used as an asset-holding vehicle?

g) Is there a sound reason for changes in the customer's ownership and control structure?

h) Does the customer request transactions that are complex, unusually or unexpectedly large, have an unusual or unexpected pattern, no apparent economic or lawful purpose, or lack a sound commercial rationale? Are there grounds to suspect that the customer is trying to evade specific thresholds such as those set out in Article 11(b) of Directive (EU) 2015/849 and national law where applicable?

i) Does the customer request unnecessary or unreasonable levels of secrecy? For example, is the customer reluctant to share CDD information, or do they appear to want to disguise the true nature of their business?

j) Can the customer's or beneficial owner's source of wealth or source of funds be easily explained, for example through their occupation, inheritance or investments? Is the explanation plausible?

k) Does the customer use the products and services they have taken out as expected when the business relationship was first established?

l) Where the customer is a non-resident, could their needs be better serviced elsewhere? Is there a sound economic and lawful rationale for the customer requesting the type of financial service sought? Firms should note that Article 16 of Directive 2014/92/EU creates a right for customers who are legally resident in the Union to obtain a basic payment account, but this right applies only to the extent that credit institutions can comply with their AML/CFT obligations as referred to in Articles 1(7) and 16(4) of Directive 2014/92/EU.

2.7. When identifying the risk associated with a customer's or beneficial owner's nature and behaviour, firms should pay particular attention to risk factors that, although not specific to terrorist financing, could point to increased TF risk, in particular in situations where other TF risk factors are also present. To this end, firms should consider at least the following risk factors:

a) Is the customer or the beneficial owner a person included in the lists of persons, groups and entities involved in terrorist acts and subject to restrictive measures[4],

[4] See for instance Council Common Position of 27 December 2001 on the application of specific measures to combat terrorism (2001/931/CFSP)(OJ L 344 , 28.12.2001, p. 0093); Council Regulation (EC) No 2580/2001 of 27 December 2001 on specific restrictive measures directed against certain persons and entities with a view to combating terrorism (OJ L

or are they known to have close personal or professional links to persons registered on such lists (for example, because they are in a relationship or otherwise live with such a person)?

b) Is the customer or the beneficial owner a person who is publicly known to be under investigation for terrorist activity or has been convicted for terrorist activity, or are they known to have close personal or professional links to such a person (for example, because they are in a relationship or otherwise live with such a person)?

c) Does the customer carry out transactions that are characterised by incoming and outgoing fund transfers from and/or to countries where groups committing terrorist offences are known to be operating, that are known to be sources of terrorist financing or that are subject to international sanctions? If so, can these transfers be explained easily through, for example, family ties or commercial relationships?

A1

d) Where the customer is a not-for-profit organisation (NPO), the firms should apply the criteria set out in the annex.

O

e) Does the customer carry out transactions characterized by large flows of money in a short period of time, involving non-profit organizations with unclear links (e.g. they are domiciled at the same physical location; they share the same representatives or employees or they hold multiple accounts under the same names)?

f) Does the customer transfer or intend to transfer funds to persons referred to in (a) and (b)?

2.8. In addition to the information sources listed in guidelines 1.30 and 1.31, firms should pay particular attention to the FATF's typologies on TF, which are regularly updated.[5]

Countries and geographical areas

344 28.12.2001, p. 70); Council Regulation (EC) No 881/2002 of 27 May 2002 imposing certain specific restrictive measures directed against certain persons and entities associated with the ISIL (Da'esh) and Al-Qaida organisations (OJ L 139 29.5.2002, p. 9). You may also consult the EU sanctions map at https://www.sanctionsmap.eu/

[5] http://www.fatf-gafi.org/publications/methodsandtrends/documents/ml-tf-risks.html

2.9. When identifying the risk associated with countries and geographical areas, firms should consider the risk related to:

a) the jurisdictions in which the customer is based or is resident, and beneficial owner is resident;

b) the jurisdictions that are the customer's and beneficial owner's main places of business; and

c) the jurisdictions to which the customer and beneficial owner have relevant personal or business links, or financial or legal interests.

2.10. Firms should note that the nature and purpose of the business relationship, or the type of business, will often determine the relative importance of individual country and geographical risk factors. For example:

a) Where the funds used in the business relationship have been generated abroad, the level of predicate offences to money laundering and the effectiveness of a country's legal system will be particularly relevant.

b) Where funds are received from, or sent to, jurisdictions where groups committing terrorist offences are known to be operating, firms should consider to what extent this could be expected to or might give rise to suspicion, based on what the firm knows about the purpose and nature of the business relationship.

c) Where the customer is a credit or financial institution, firms should pay particular attention to the adequacy of the country's AML/CFT regime and the effectiveness of AML/CFT supervision.

d) Where the customer is a trust or any other type of legal arrangement, or has a structure or functions similar to trusts such as, fiducie, fideicomiso, Treuhand, firms should take into account the extent to which the country in which the customer and, where applicable, the beneficial owner are registered effectively complies with international tax transparency and information sharing standards.

2.11. Risk factors firms should consider when identifying the effectiveness of a jurisdiction's AML/CFT regime include:

a) Has the country been identified by the Commission as having strategic deficiencies in its AML/CFT regime, in line with Article 9 of Directive (EU) 2015/849? In those cases, firms should refer to guideline 4.53 to 4.57 for guidance.

b) Does the country's law prohibit the implementation of group-wide policies and procedures and in particular are there any situations in which the Commission delegated Regulation (EU) 2019/758 should be applied?

c) Is there information from more than one credible and reliable source about the quality of the jurisdiction's AML/CFT controls, including information about the quality and effectiveness of regulatory enforcement and oversight? Examples of possible sources include mutual evaluation reports by the Financial Action Task Force (FATF) or FATF-style Regional Bodies (FSRBs) (a good starting point is the executive summary and key findings and the assessment of compliance with Recommendations 10, 26 and 27 and Immediate Outcomes 3 and 4), the FATF's list of high-risk and non- cooperative jurisdictions, International Monetary Fund (IMF) assessments and Financial Sector Assessment Programme (FSAP) reports. Firms should note that membership of the FATF or an FSRB (e.g. Moneyval) does not, of itself, mean that the jurisdiction's AML/CFT regime is adequate and effective.

2.12. Firms should note that Directive (EU) 2015/849 does not recognise the 'equivalence' of third countries and that EU Member States' lists of equivalent jurisdictions are no longer being maintained. To the extent permitted by national legislation, firms should be able to identify lower risk jurisdictions in line with these guidelines and Annex II of Directive (EU) 2015/849.

2.13. Risk factors firms should consider when identifying the level of terrorist financing risk associated with a jurisdiction include:

a) Is there information, for example from law enforcement or credible and reliable open media sources, suggesting that a jurisdiction provides funding or support for terrorist activities, either from official sources, or from organised groups or organisations within that jurisdiction?

b) Is there information, for example from law enforcement or credible and reliable open media sources, suggesting that groups committing terrorist offences are known to be operating in the country or territory?

c) Is the jurisdiction subject to financial sanctions, embargoes or measures that are related to terrorism, financing of terrorism or proliferation issued by, for example, the United Nations or the European Union?

2.14. Risk factors firms should consider when identifying a jurisdiction's level of transparency and tax compliance include:

a) Is there information from more than one credible and reliable source that the country has been deemed compliant with international tax transparency and information sharing standards? Is there evidence that relevant rules are

effectively implemented in practice? Examples of possible sources include reports by the Global Forum on Transparency and the Exchange of Information for Tax Purposes of the Organisation for Economic Co-operation and Development (OECD), which rate jurisdictions for tax transparency and information sharing purposes; assessments of the jurisdiction's commitment to automatic exchange of information based on the Common Reporting Standard; assessments of compliance with FATF Recommendations 9, 24 and 25 and Immediate Outcomes 2 and 5 by the FATF or FSRBs; assessments conducted with regard to the EU list of non-cooperative jurisdictions for tax purposes; and IMF assessments (e.g. IMF staff assessments of offshore financial centres).

b) Has the jurisdiction committed to, and effectively implemented, the Common Reporting Standard on Automatic Exchange of Information, which the G20 adopted in 2014?

c) Has the jurisdiction put in place reliable and accessible beneficial ownership registers?

2.15. Risk factors firms should consider when identifying the risk associated with the level of predicate offences to money laundering include:

a) Is there information from credible and reliable public sources about the level of predicate offences to money laundering listed in Article 3(4) of Directive (EU) 2015/849, for example corruption, organised crime, tax crime and serious fraud? Examples include corruption perception indices; OECD country reports on the implementation of the OECD's anti-bribery convention; and the United Nations Office on Drugs and Crime World Drug Report.

b) Is there information from more than one credible and reliable source about the capacity of the jurisdiction's investigative and judicial system effectively to investigate and prosecute these offences?

Products, services and transactions risk factors

2.16. When identifying the risk associated with their products, services or transactions, firms should consider the risk related to:

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

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

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

2.17. Risk factors firms should consider when identifying the risk associated with a product, service or transaction's transparency include:

a) To what extent do products or services allow the customer or beneficial owner or beneficiary structures to remain anonymous, or facilitate hiding their identity? Examples of such products and services include bearer shares, fiduciary deposits, offshore vehicles and certain trusts, and legal entities such as foundations that can be structured in such a way as to take advantage of anonymity and allow dealings with shell companies or companies with nominee shareholders.

b) To what extent is it possible for a third party that is not part of the business relationship to give instructions, for example in the case of certain correspondent banking relationships?

2.18. Risk factors firms should consider when identifying the risk associated with a product, service or transaction's complexity include:

a) How complex is the transaction and does it involve multiple parties or multiple jurisdictions, for example in the case of certain trade finance transactions? Are transactions straightforward, for example are regular payments made into a pension fund?

b) To what extent do products or services allow payments from third parties or accept overpayments where this is would not normally be expected? Where third party payments are expected, does the firm know the third party's identity, for example is it a state benefit authority or a guarantor? Or are products and services funded exclusively by fund transfers from the customer's own account at another financial institution that is subject to AML/CFT standards and oversight that are comparable to those required under Directive (EU) 2015/849?

c) Does the firm understand the risks associated with its new or innovative product or service, in particular where this involves the use of new technologies or payment methods?

2.19. Risk factors firms should consider when identifying the risk associated with a product, service or transaction's value or size include:

a) To what extent are products or services cash intensive, as are many payment services but also certain current accounts?

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

Delivery channel risk factors

2.20. When identifying the risk associated with the way in which the customer obtains the products or services they require, firms should consider the risk related to:

a) the extent to which the business relationship is conducted on a non-face-to-face basis; and

b) any introducers or intermediaries the firm might use and the nature of their relationship with the firm.

2.21. When assessing the risk associated with the way in which the customer obtains the products or services, firms should consider a number of factors including:

a) whether the customer is physically present for identification purposes. If they are not, whether the firm

i. used a reliable form of non-face-to-face CDD; and

ii. took steps to prevent impersonation or identity fraud.

Firms should apply Guidelines 4.29 to 4.31 in those situations.

b) whether the customer has been introduced by another part of the same financial group and, if so, to what extent the firm can rely on this introduction as reassurance that the customer will not expose the firm to excessive ML/TF risk, and what the firm has done to satisfy itself that the group entity applies CDD measures to European Economic Area (EEA) standards in line with Article 28 of Directive (EU) 2015/849;

c) whether the customer has been introduced by a third party, for example a bank that is not part of the same group or an intermediary, and if so

i. whether the third party is a regulated person subject to AML obligations that are consistent with those of Directive (EU) 2015/849, and whether the third party is a financial institution or its main business activity is unrelated to financial service provision;

ii. whether the third party applies CDD measures, keeps records to EEA standards, is supervised for compliance with comparable AML/CFT obligations in line with Article 26 of Directive (EU) 2015/849, and whether there are any indications that the third party's level of compliance with applicable AML/CFT legislation or regulation is inadequate, for example whether the third party has been sanctioned for breaches of AML/CFT obligations;

iii. whether they are based in a jurisdiction associated with higher ML/TF risk. Where a third party is based in a high-risk third country that the CEU Commission has identified as having strategic deficiencies, firms must not rely on that third party. However, to the extent permitted by national legislation, reliance may be possible provided that the intermediary is a branch or majority-owned subsidiary of another firm established in the Union, and the firm is confident that the intermediary fully complies with group-wide policies and procedures in line with Article 45 of Directive (EU) 2015/849.[6]

iv. what the firm has done to satisfy itself that:

a. the third party always provides the necessary identity documentation;

b. the third party will provide, immediately upon request, relevant copies of identification and verification data or electronic data referred to, *inter alia*, in Article 27 of Directive (EU) 2015/849;

c. the quality of the third party's CDD measures is such that it can be relied upon; and

d. the level of CDD applied by the third party is commensurate to the ML/TF risk associated with the business relationship, considering that the third party will have applied CDD measures for its own purposes and, potentially, in a different context.

d) whether the customer has been introduced through a tied agent, that is, without direct firm contact, and to what extent the firm can be satisfied that the agent has obtained enough information to ensure that the firm knows its customer and the level of risk associated with the business relationship;

e) whether independent or tied agents are used, to what extent they are involved on an ongoing basis in the conduct of business, and how this affects the firm's knowledge of the customer and ongoing risk management;

f) To the extent permitted by national legislation, when the firm uses an outsourced service provider for aspects of its AML/CFT obligations, whether it has considered whether the outsourced service provider is an obliged entity, and whether it has addressed the risks set out in the EBA's Guidelines on outsourcing (EBA/GL/2019/02), where those Guidelines are applicable.

[6] Article 26(2) of Directive (EU) 2015/849

Guideline 3: Assessing ML/TF risk

3.1. Firms should use the risk factors they have identified to assess the overall level of ML/TF risk.

Taking a holistic view

3.2. Firms should take a holistic view of the ML/TF risk factors they have identified that, together, will determine the level of ML/TF risk associated with a business relationship, an occasional transaction, or their business.

3.3. Firms should note that, unless Directive (EU) 2015/849 or national legislation states otherwise, the presence of isolated risk factors does not necessarily move a relationship into a higher or lower risk category.

Weighting risk factors

3.4. When assessing ML/TF risk, firms may decide to weight factors differently depending on their relative importance.

3.5. When weighting risk factors, firms should make an informed judgement about the relevance of different risk factors in the context of a business relationship, an occasional transaction or their business. This often results in firms allocating different 'scores' to different factors; for example, firms may decide that a customer's personal links to a jurisdiction associated with higher ML/TF risk is less relevant in light of the features of the product they seek.

3.6. Ultimately, the weight given to each of these factors is likely to vary from product to product and customer to customer (or category of customer) and from one firm to another. When weighting risk factors, firms should ensure that:

a) weighting is not unduly influenced by just one factor;

b) economic or profit considerations do not influence the risk rating;

c) weighting does not lead to a situation where it is impossible for any business relationship to be classified as high risk;

d) the provisions of Directive (EU) 2015/849 or national legislation regarding situations that always present a high money laundering risk cannot be over-ruled by the firm's weighting; and

e) they are able to over-ride any automatically generated risk scores where necessary. The rationale for the decision to over-ride such scores should be documented appropriately.

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

Categorising risk

3.8. Firms should decide on the most appropriate way to categorise risk. This will depend on the nature and size of the firm's business and the types of ML/TF risk it is exposed to. Although firms often categorise risk as high, medium and low, other categorisations are possible.

3.9. Following its risk assessment, and having taken into account both inherent risks and any mitigants it has identified, a firm should categorise its business lines as well as their business relationships and occasional transactions according to the perceived level of ML/TF risk.

Guideline 4: CDD measures to be applied by all firms

4.1. A firm's business-wide and individual risk assessments should help it identify where it should focus its ML/TF isk management efforts, both at customer take-on and for the duration of the business relationship.

4.2. Firms should ensure that their AML/CFT policies and procedures build on, and reflect, their risk assessment.

4.3. They should also ensure that their AML/CFT policies and procedures are readily available, applied, effective, and understood by all relevant staff.

4.4. When complying with their obligation under Article 8 of Directive 2015/849 to obtain approval for their AML/CFT policies, controls and procedures from their senior management, firms should ensure that senior management have access to sufficient data, including the firm's business-wide ML/TF risk assessment, to take an informed view on the adequacy and effectiveness of these policies and procedures and in particular their CDD policies and procedures.

Customer due diligence

4.5. CDD measures should help firms better understand the risk associated with individual business relationships and occasional transactions.

4.6. Firms must apply each of the CDD measures set out in Article 13(1) of Directive (EU) 2015/849 but may determine the extent of each of these measures on a risk- sensitive basis.

4.7. Firms should set out clearly, in their policies and procedures,

a) who the customer and, where applicable, beneficial owner is for each type of customer and category of products and services, and whose identity has to be verified for CDD purposes. Firms should refer to the sectoral guidance in Title II of these guidelines, which has further detail on the identification of customers and their beneficial owners.

b) what constitutes an occasional transaction in the context of their business and at what point a series of one-off transactions amounts to a business relationship, rather than an occasional transaction, taking into consideration factors such as the frequency or regularity with which the customer returns for occasional transactions, and the extent to which the relationship is expected to have, or appears to have, an element of duration. Firms should note that the monetary threshold in Article 11 (b) of Directive (EU) 2015/847 is relevant only to the extent that it triggers an absolute requirement to apply CDD measures; a series of occasional transactions can be a business relationship even where that threshold is not reached;

c) what the appropriate level and type of CDD that they will apply to individual business relationships and occasional transactions;

d) how they expect the identity of the customer and, where applicable, the beneficial owner to be verified and how they expect the nature and purpose of the business relationship to be established;

e) which level of monitoring is to be applied in what circumstances;

f) how, and in which situations, weaker forms of identification and verification of identity can be compensated for by enhanced monitoring; and

g) the firm's risk appetite.

4.8. As set out in Article 13(4) of Directive (EU) 2015/849, firms should be able to demonstrate to their competent authority that the CDD measures they have applied are commensurate to the ML/TF risks.

Financial inclusion and de-risking

4.9. 'De-risking' refers to a decision taken by firms to no longer offer services to some categories of customers associated with higher ML/TF risk. As the risk associated with individual business relationships will vary, even within one category, the application of a risk-based approach does not require firms to refuse, or terminate, business relationships with entire

categories of customers that are considered to present higher ML/TF risk. Firms should carefully balance the need for financial inclusion with the need to mitigate ML/TF risk.

4.10. As part of this, firms should put in place appropriate and risk-sensitive policies and procedures to ensure that their approach to applying CDD measures does not result in unduly denying legitimate customers access to financial services., Where a customer has legitimate and credible reasons for being unable to provide traditional forms of identity documentation, firms should consider mitigating ML/TF risk in other ways, including by

a) Adjusting the level and intensity of monitoring in a way that is commensurate to the ML/TF risk associated with the customer, including the risk that a customer who may have provided a weaker form of identity documentation may not be who they claim to be; and

b) Offering only basic financial products and services, which restrict the ability of users to abuse these products and services for financial crime purposes. Such basic products and services may also make it easier for firms to identify unusual transactions or patterns of transactions, including the unintended use of the product; but it is important that any limits be proportionate and do not unreasonably or unnecessarily limit customers' access to financial products and services.

4.11. Firms may wish to refer to the EBA's Opinion on the application of customer due diligence measures to customers who are asylum seekers from higher-risk third countries or territories (EBA-OP-2016-07).

Beneficial owners

4.12. When discharging their obligations set out in Article 13(1)(b) of Directive (EU) 2015/849 to understand the customer's ownership and control structure firms should take at least the followings steps :

a) Firms should ask the customer who their beneficial owners are;

b) Firms should document the information obtained.

c) Firms should then take all necessary and reasonable measures to verify the information: to achieve this, firms should consider using beneficial ownership registers where available.

d) Steps b) and c) should be applied on a risk-sensitive basis.

Beneficial ownership registers

4.13. Firms should be mindful that using information contained in beneficial ownership registers does not, in itself, fulfil their duty to take adequate and risk-sensitive measures to identity the beneficial owner and verify their identity. Firms may have to take additional steps to identify and verify the beneficial owner, in particular where the risk associated with the business relationship is increased or where the firm has doubts that the person listed in the register is the ultimate beneficial owner.

Control through other means

4.14. The requirement to identify, and take all necessary and reasonable measures to verify the identity of the beneficial owner relates only to the natural person who ultimately owns or controls the customer. However, to comply with their obligations under Article 13 of Directive (EU) 2015/849, firms should also take reasonable measures to understand the customer's ownership and control structure.

4.15. The measures firms take to understand the customer's ownership and control structure should be sufficient so that the firm can be reasonably satisfied that it understands the risk associated with different layers of ownership and control. In particular, firms should be satisfied that,

a) the customer's ownership and control structure is not unduly complex or opaque; or

b) complex or opaque ownership and control structures have a legitimate legal or economic reason.

4.16. To meet their obligations under Article 33 (1) of Directive (EU) 2015/849, firms should report to the FIU if the customer's ownership and control structure give rise to suspicion and they have reasonable grounds to suspect that the funds may be the proceeds of criminal activity or are related to terrorist financing.

4.17. Firms should pay particular attention to persons who may exercise 'control through other means' under Article 3(6) (a)(i) of Directive (EU) 2015/849. Examples of 'control through other means' firms should consider include, but are not limited to:

a) control without direct ownership, for example through close family relationships, or historical or contractual associations;

b) using, enjoying or benefiting from the assets owned by the customer;

c) responsibility for strategic decisions that fundamentally affect the business practices or general direction of a legal person.

4.18. Firms should decide, on a risk-sensitive basis, whether to verify the customer's ownership and control structure.

Identifying the customer's senior managing officials

4.19. Where the customer is a legal entity, firms should make every effort to identify the beneficial owner as defined in Article 3(6)(a) (i) of Directive (EU) 2015/849.

4.20. Firms should resort to identifying the customer's senior managing officials as beneficial owners only if:

a) They have exhausted all possible means of identifying the natural person who ultimately owns or controls the customer;

b) Their inability to identify the natural person who ultimately owns or controls the customer does not give rise to suspicions of ML/TF; and

c) They are satisfied that the reason given by the customer as to why the natural person who ultimately owns or controls the customer cannot be identified is plausible.

4.21. When deciding which senior managing official, or which senior managing officials, to identify as beneficial owner, firms should consider who has ultimate and overall responsibility for the customer and takes binding decisions on the customer's behalf.

4.22. In those cases, firms should clearly document their reasons for identifying the senior manager, rather than the customer's beneficial owner, and must keep records of their actions[7].

Identifying the beneficial owner of a public administration or a state-owned enterprises

4.23. Where the customer is a public administration or a state-owned enterprise, firms should follow the guidance in guidelines 4.21 and 4.22 to identify the senior managing official.

4.24. In those cases, and in particular where the risk associated with the relationship is increased, for example because the state-owned enterprise is from a country associated with high levels of corruption, firms should take risk-sensitive steps to establish that the person they have identified as the beneficial owner is properly authorised by the customer to act on the customer's behalf.

4.25. Firms should also have due regard to the possibility that the senior managing official of the customer may be a PEP. Should this be the case, firms must apply EDD measures to that senior managing official in line with Article 18 of Directive (EU) 2015/849, and assess whether the extent to which the PEP can influence the customer gives rise to increased ML/TF risk and whether it may be necessary to apply EDD measures to the customer.

[7] Article 3(6)(a)(ii) of Directive (EU) 2015/849

Evidence of identity

4.26. To comply with their obligations under Article 13(1)(a) and (b) of Directive (EU) 2015/849, firms should verify their customer's identity and, where applicable, beneficial owners' identity, on the basis of reliable and independent information and data, whether this is obtained remotely, electronically or in documentary form.

4.27. Firms should set out in their policies and procedures which information and data they will treat as reliable and independent for CDD purposes. As part of this, firms should consider

a) What makes data or information reliable. Firms should consider different degrees of reliability, which they should determine based on

i. the extent to which the customer had to undergo certain checks to obtain the information or data provided;

ii. the official status, if any, of the person or institution that carried out those checks;

iii. the level of assurance associated with any digital ID system used; and

iv. the ease with which the identity information or data provided can be forged.

b) What makes data or information independent. Firms should consider different degrees of independence, which they should determine based on the extent to which the person or institution that originally issued or provided the data or information:

i. is linked to the customer through direct personal, professional or family ties; and

ii. could have been unduly influenced by the customer.

In most cases, firms should be able to treat government-issued information or data as providing the highest level of independence and reliability.

4.28. Firms should assess the risks associated with each type of evidence provided and the method of identification and verification used and ensure that the method and type chosen is commensurate with the ML/TF risk associated with the customer.

Non-face to face situations

4.29. To perform their obligations under Article 13(1) of Directive (EU) 2015/849, where the business relationship is initiated, established, or conducted in non-face to face situations or an occasional transaction is done in non-face to face situations, firms should:

a) take adequate measures to be satisfied that the customer is who he claims to be; and

b) assess whether the non-face to face nature of the relationship or occasional transaction gives rise to increased ML/TF risk and if so, adjust their CDD measures accordingly. When assessing the risk associated with non-face to face relationships, firms should have regard to the risk factors set out in Guideline 2.

4.30. Where the risk associated with a non-face to face relationship or an occasional transaction is increased, firms should apply EDD measures in line with Guidelines 4.46. Firms should consider in particular whether enhanced measures to verify the identity of the customer or enhanced ongoing monitoring of the relationship would be appropriate.

4.31. Firms should have regard to the fact that the use of electronic means of identification does not of itself give rise to increased ML/TF risk, in particular where these electronic means provide a high level of assurance under Regulation (EU) 910/2014.

Using innovative technological means to verify identity

4.32. Directive (EU) 2015/849 is technology neutral and firms may choose to use electronic or documentary means, or a combination thereof, to evidence their customers' identity; but pursuant to Article 13(1)(a) of Directive (EU) 2015/849 firms should make sure that this evidence is based on data or information from reliable and independent sources.

4.33. Firms that use or intend to use innovative technological means for identification and verification purposes should assess the extent to which the use of innovative technological solutions can address, or might exacerbate, the ML/TF risks, in particular in non-face to face situations. As part of their assessment, firms should have a clear view on:

a) ICT and security risks, in particular the risk that the innovative solution may be unsuitable or unreliable or could be tampered with;

b) qualitative risks, in particular the risk that the sources of information used for verification purposes are not sufficiently independent and reliable and therefore fall short of Union law or national law; and the risk that the extent of identity verification provided by the innovative solution is not commensurate with the level of ML/TF risk associated with the business relationship;

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

d) impersonation fraud risks, that is, the risk that a customer is not who they claim to be. Firms should also consider the risk that the person is not a real person.

4.34. Firms that use an external provider, rather than develop their own innovative solution in-house, remain ultimately responsible for meeting their CDD obligations. They should be clear about their relationship with the innovative solution provider (e.g. whether it is an

outsourcing relationship, or whether the use of the innovative solution constitutes a form of reliance on a third party as per Section 4 of Directive (EU) 2015/849), and take sufficient steps to be satisfied that the innovative solution provider:

a) is registered with relevant national authorities to access and store personal data to EU legal standards in compliance with Regulation (EU) 2016/679 (General Data Protection Regulation (GDPR)[8] and legislation by which the GDPR has been implemented;

b) accesses and uses a sufficient range of data from different sources and across time, having regard to the following elements in particular

i. electronic evidence based on a customer's passport is unlikely to be sufficient in a non-face to face context without accompanying checks to ensure that the customer is who they say they are, and that the document has not been tampered with; and

ii. a single data source or a single point in time is unlikely to be enough to meet verification standards in most situations

c) is contractually bound to comply with duties required by their agreement and binding norms of Union Law and national law, and to inform the firm immediately should anything change; and

d) operates transparently, so that the firm knows at all times which checks were carried out, which sources were used, what the results were and how robust these results were.

4.35. Where the external provider is a firm established in a third country, the firm should ensure that it understands the legal risks and operational risks and data protection requirements associated therewith and mitigates those risks effectively.

4.36. Firms should be prepared to demonstrate to their competent authority that the use of a particular innovative solution is appropriate.

4.37. Firms may wish to refer to the ESAs' 2018 Joint Opinion on the use of innovative solutions in the customer due diligence process, which has further detail on these points.

Establishing the nature and purpose of the business relationship

4.38. The measures firms take to establish the nature and purpose of the business relationship should be commensurate to the risk associated with the relationship and sufficient to enable

[8] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation),(OJ L 119, 4.5.2016, p. 1).

the firm to understand who the customer is, and who the customer's beneficial owners are. Firms should at least take steps to understand:

a) The nature of the customer's activities or business;

b) Why the customer has chosen the firm's products and services;

c) The value and sources of funds that will be flowing through the account;

d) How the customer will be using the firm's products and services;

e) Whether the customer has other business relationships with other parts of the firm or its wider group, and the extent to which this affects the firm's understanding of the customer; and

f) What constitutes 'normal' behaviour for this customer or category of customers.

4.39. Firms should refer to the risk factors in guidelines 2.4 to 2.6 of these guidelines.

Simplified customer due diligence

4.40. To the extent permitted by national legislation, firms may apply SDD measures in situations where the ML/TF risk associated with a business relationship has been assessed as low. SDD is not an exemption from any of the CDD measures; however, firms may adjust the amount, timing or type of each or all of the CDD measures in a way that is commensurate to the low risk they have identified.

4.41. SDD measures firms may apply include but are not limited to:

a) the timing of CDD, for example where the product or transaction sought has features that limit its use for ML/TF purposes, for example by:

i. verifying the customer's or beneficial owner's identity during the establishment of the business relationship; or

ii. verifying the customer's or beneficial owner's identity once transactions exceed a defined threshold or once a reasonable time limit has lapsed. Firms must make sure that:

a. this does not result in a *de facto* exemption from CDD, that is, firms must ensure that the customer's or beneficial owner's identity will ultimately be verified;

b. the threshold or time limit is set at a reasonably low level (although, with regard to terrorist financing, firms should note that a low threshold alone may not be enough to reduce risk);

c. they have systems in place to detect when the threshold or time limit has been reached; and

d. they do not defer CDD or delay obtaining relevant information about the customer where applicable legislation, for example Regulation (EU) 2015/847 or provisions in national legislation, require that this information be obtained at the outset.

b) adjusting the quantity of information obtained for identification, verification or monitoring purposes, for example by:

i. verifying identity on the basis of information obtained from one reliable, credible and independent document or data source only; or

ii. assuming the nature and purpose of the business relationship because the product is designed for one particular use only, such as a company pension scheme or a shopping center gift card.

c) adjusting the quality or source of information obtained for identification, verification or monitoring purposes, for example by:

i. accepting information obtained from the customer rather than an independent source when verifying the beneficial owner's identity (note that this is not permitted for the verification of the customer's identity); or

ii. where the risk associated with all aspects of the relationship is very low, relying on the source of funds to meet some of the CDD requirements, for example where the funds are state benefit payments or where the funds have been transferred from an account in the customer's name at an EEA firm;

d) adjusting the frequency of CDD updates and reviews of the business relationship, for example carrying these out only when trigger events occur such as the when the customer looks to take out a new product or service or when a certain transaction threshold is reached; firms must make sure that this does not result in a *de facto* exemption from keeping CDD information up-to-date.

e) adjusting the frequency and intensity of transaction monitoring, for example by monitoring transactions above a certain threshold only. Where firms choose to

do this, they must ensure that the threshold is set at a reasonable level and that they have systems in place to identify linked transactions that, together, would exceed that threshold.

4.42. Title II lists additional SDD measures that may be of particular relevance in different sectors.

4.43. The information a firm obtains when applying SDD measures must enable the firm to be reasonably satisfied that its assessment that the risk associated with the relationship is low is justified. It must also be sufficient to give the firm enough information about the nature of the business relationship to identify any unusual or suspicious transactions. SDD does not exempt an institution from reporting suspicious transactions to the FIU.

4.44. Where there are indications that the risk may not be low, for example where there are grounds to suspect that ML/TF is being attempted or where the firm has doubts about the veracity of the information obtained, SDD must not be applied.[9] Equally, where specific high-risk scenarios apply and there is an obligation to conduct EDD, SDD must not be applied.

Enhanced customer due diligence

4.45. Pursuant to Articles 18 to 24 of Directive (EU) 2015/849, firms must apply EDD measures in higher risk situations to manage and mitigate those risks appropriately. EDD measures cannot be substituted for regular CDD measures but must be applied in addition to regular CDD measures.

4.46. Directive (EU) 2015/849 lists specific cases that firms must always treat as higher risk:

a) where the customer, or the customer's beneficial owner, is a PEP (Articles 20 to 24);

b) where a firm enters into a correspondent relationship involving the execution of payments with a third-country institution (Article 19);

c) where a firm maintains a business relationship or carries out a transaction involving high-risk third countries (Article 18(1)); and

d) all transactions that are

i. complex;

ii. unusually large;

iii. conducted in an unusual pattern; or

[9] Article 11(e) and (f) and Article 15(2) of Directive (EU) 2015/849.

iv. without obvious economic or lawful purpose (Article 18(2)).

4.47. Directive (EU) 2015/849 sets out specific EDD measures that firms must apply:

a) where the customer, or the customer's beneficial owner, is a PEP;

b) where the business relationship or transaction involves a high risk third country identified by the Commission pursuant to Article 9(2) of Directive (EU) 2015/849;

c) with respect to correspondent relationships involving the execution of payments with respondents from third countries; and

d) with respect to all transactions that are either complex, unusually large, conducted in an unusual pattern or do not have an apparent economic or lawful purpose.

Firms should apply additional EDD measures in those situations where this is commensurate to the ML/TF risk they have identified.

Politically Exposed Persons

4.48. When putting in place risk-sensitive policies and procedures to identify PEPs, firms should have regard to the list of prominent public functions published by the Commission pursuant to Article 20a(3) of Directive (EU) 2015/849 and ensure that holders of these functions are identified. This list applies to prominent functions in the EU; when determining how to identify PEPs from third countries, firms should instead refer to the list of functions in Article 3(9) of Directive (EU) 2015/849 and adjust this list on a case-by-case basis.

4.49. Firms that use commercially available PEP lists should ensure that information on these lists is up to date and that they understand the limitations of those lists. Firms should take additional measures where necessary, for example in situations where the screening results are inconclusive or not in line with the firm's expectations.

4.50. Firms that have identified that a customer or beneficial owner is a PEP must always:

a) Take adequate measures to establish the source of wealth and the source of funds to be used in the business relationship in order to allow the firm to satisfy itself that it does not handle the proceeds from corruption or other criminal activity. The measures firms should take to establish the PEP's source of wealth and the source of funds will depend on the degree of high risk associated with the business relationship. Firms should verify the source of wealth and the source of funds on the basis of reliable and independent data, documents or information where the risk associated with the PEP relationship is particularly high.

b) Obtain senior management approval for entering into, or continuing, a business relationship with a PEP. The appropriate level of seniority for sign-off should be determined by the level of increased risk associated with the business relationship, and the senior manager approving a PEP business relationship should have sufficient seniority and oversight to take informed decisions on issues that directly impact the firm's risk profile.

c) When considering whether to approve a PEP relationship, senior management should base their decision on the level of ML/TF risk the firm would be exposed to if it entered into that business relationship and how well equipped the firm is to manage that risk effectively.

d) Apply enhanced ongoing monitoring of both transactions and the risk associated with the business relationship. Firms should identify unusual transactions and regularly review the information they hold to ensure that any new or emerging information that could affect the risk assessment is identified in a timely fashion. The frequency of ongoing monitoring should be determined by the level of high risk associated with the relationship.

4.51. Pursuant to Article 20(b) of Directive (EU) 2015/849, firms must apply all of these measures to PEPs, their family members and known close associates and should adjust the extent of these measures on a risk-sensitive basis.

4.52. Firms should ensure that the measures they put in place to comply with the Directive (EU) 2015/849and with these guidelines in respect of PEPs do not result in PEP customers being unduly denied access to financial services.

High-risk third countries

4.53. With respect to a business relationship or transaction involving high-risk third countries as set out in Article 9(2) of Directive (EU) 2015/849, firms should ensure that they apply, as a minimum, the EDD measures set out in Article 18a(1) and, where applicable, the measures set out in Article 18 a(2) of Directive (EU) 2015/849.

4.54. Firms should apply the measures listed in guideline 4.53 and should adjust the extent of these measures on a risk-sensitive basis.

4.55. A business relationship or transaction always involves a high risk third country if

a) the funds were generated in a high risk third country;

b) the funds are received from a high risk third country;

c) the destination of funds is a high risk third country;

d) the firm is dealing with a natural person or legal entity resident or established in a high risk third country; or

e) the firm is dealing with a trustee established in a high risk third country or with a trust governed under the law of a high risk third country.

4.56. When performing CDD measures or during the course of a business relationship, firms should ensure that they also apply the EDD measures set out in Article 18a(1) and, where applicable, the measures set out in Article 18a(2) of Directive (EU) 2015/849, where firms determine that

a) the transaction passes through a high-risk third country, for example because of where the intermediary payment services provider is based; or

b) a customer's beneficial owner is resident in a high-risk third country.

4.57. Notwithstanding guidelines 4.54 and 4.56, firms should carefully assess the risk associated with business relationships and transactions where

a) the customer is known to maintain close personal or professional links with a high-risk third country; or

b) beneficial owner(s) is/are known to maintain close personal or professional links with a high-risk third country.

In those situations, firms should take a risk-based decision on whether or not to apply the measures listed in Article 18a) of Directive (EU) 2015/849, EDD measures or regular CDD measures.

Correspondent relationships

4.58. To comply with Article 19 of Directive (EU) 2015/849, firms must take specific EDD measures where they have a cross-border correspondent relationship with a respondent based in a third country. Firms must apply all of these measures and should adjust the extent of these measures on a risk-sensitive basis.

4.59. Firms should refer to Title II for guidelines on EDD in relation to correspondent banking relationships; these guidelines may also be useful for firms in other correspondent relationships.

Unusual transactions

4.60. Firms should put in place adequate policies and procedures to detect unusual transactions or patterns of transactions. Where a firm detects such transactions, it must apply EDD measures. Transactions may be unusual because:

a) they are larger than what the firm would normally expect based on its knowledge of the customer, the business relationship or the category to which the customer belongs;

b) they have an unusual or unexpected pattern compared with the customer's normal activity or the pattern of transactions associated with similar customers, products or services; or

c) they are very complex compared with other, similar, transactions associated with similar customer types, products or services, and the firm is not aware of an economic rationale or lawful purpose or doubts the veracity of the information it has been given.

4.61. These EDD measures should enable the firm to determine whether these transactions give rise to suspicion and must at least include:

a) taking reasonable and adequate measures to understand the background and purpose of these transactions, for example by establishing the source and destination of the funds or finding out more about the customer's business to ascertain the likelihood of the customer making such transactions; and

b) monitoring the business relationship and subsequent transactions more frequently and with greater attention to detail. A firm may decide to monitor individual transactions where this is commensurate to the risk it has identified.

Other high-risk situations

4.62. In all other high risk situations, firms should take an informed decision about which EDD measures are appropriate for each high-risk situation. The appropriate type of EDD, including the extent of the additional information sought, and of the increased monitoring carried out, will depend on the reason why an occasional transaction or a business relationship was classified as high risk.

4.63. Firms are not required to apply all the EDD measures listed below in all cases. For example, in certain high-risk situations it may be appropriate to focus on enhanced ongoing monitoring during the course of the business relationship.

4.64. EDD measures firms should apply may include:

a) Increasing the quantity of information obtained for CDD purposes as follows:

i. Information about the customer's or beneficial owner's identity, or the customer's ownership and control structure, to be satisfied that the risk associated with the relationship is well understood. This may include obtaining and assessing information about the customer's or beneficial owner's reputation

and assessing any negative allegations against the customer or beneficial owner. Examples include:

a. information about family members and close business partners;

b. information about the customer's or beneficial owner's past and present business activities; and

c. adverse media searches.

ii. Information about the intended nature of the business relationship to ascertain that the nature and purpose of the business relationship is legitimate and to help firms obtain a more complete customer risk profile. This may include obtaining information on:

a. the number, size and frequency of transactions that are likely to pass through the account, to enable the firm to spot deviations that might give rise to suspicion (in some cases, requesting evidence may be appropriate);

b. why the customer is looking for a specific product or service, in particular where it is unclear why the customer's needs cannot be met better in another way, or in a different jurisdiction;

c. the destination of funds;

d. the nature of the customer's or beneficial owner's business, to enable the firm to better understand the likely nature of the business relationship.

b) Increasing the quality of information obtained for CDD purposes to confirm the customer's or beneficial owner's identity including by:

i. requiring the first payment to be carried out through an account verifiably in the customer's name with a bank subject to CDD standards that are not less robust than those set out in Chapter II of Directive (EU) 2015/849; or

ii. establishing that the customer's wealth and the funds that are used in the business relationship are not the proceeds of criminal activity and that the source of wealth and source of funds are consistent with the firm's knowledge of the customer and the nature of the business relationship. In some cases, where the risk associated with the relationship is particularly high, verifying the source of wealth and the

source of funds may be the only adequate risk mitigation tool. The source of funds or wealth can be verified, *inter alia*, by reference to VAT and income tax returns, copies of audited accounts, pay slips, public deeds or independent media reports. Firms should have regard to the fact that funds from legitimate business activity may still constitute money laundering or terrorist financing as set out in paragraphs (3) to (5) of Article 1 of Directive (EU) 2015/849.

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

i. increasing the frequency of reviews of the business relationship to ascertain whether the customer's risk profile has changed and whether the risk remains manageable;

ii. obtaining the approval of senior management to commence or continue the business relationship to ensure that senior management are aware of the risk their firm is exposed to and can take an informed decision about the extent to which they are equipped to manage that risk;

iii. reviewing the business relationship on a more regular basis to ensure any changes to the customer's risk profile are identified, assessed and, where necessary, acted upon; or

iv. conducting more frequent or in-depth transaction monitoring to identify any unusual or unexpected transactions that might give rise to suspicion of ML/TF. This may include establishing the destination of funds or ascertaining the reason for certain transactions.

4.65. Title II lists additional EDD measures that may be of particular relevance in different sectors.

Other considerations

4.66. Firms should not enter into a business relationship if they are unable to comply with their CDD requirements, if they are not satisfied that the purpose and nature of the business relationship are legitimate or if they are not satisfied that they can effectively manage the risk that they may be used for ML/TF purposes. Where such a business relationship already exists, firms should terminate it or suspend transactions until it can be terminated, subject to instructions from law enforcement, where applicable.

4.67. Where firms have reasonable grounds to suspect that ML/TF is being attempted, firms must report this to their FIU.

4.68. Firms should note that the application of a risk-based approach does not of itself require them to refuse, or terminate, business relationships with entire categories of customers that they associate with higher ML/TF risk, as the risk associated with individual business relationships will vary, even within one category.

Monitoring

4.69. Pursuant to Article 13 of Directive (EU) 2015/849, firms should monitor their business relationships with their customers.

4.70. Monitoring should include:

a. Monitoring of transactions to ensure that these are in line with the customer's risk profile, their financial situation, and the firm's wider knowledge of the customer to detect unusual or suspicious transactions; and

b. keeping the documents, data or information they hold up to date, with a view to understanding whether the risk associated with the business relationship has changed and to ascertain that the information that forms the basis for ongoing monitoring is accurate.

4.71. Firms should determine the frequency and intensity of monitoring on a risk-sensitive basis, taking into account the nature, size and complexity of their business and the level of risk to which they are exposed.

Transaction monitoring

4.72. Firms should ensure that their approach to transaction monitoring is effective and appropriate.

4.73. An effective transaction monitoring system relies on up-to-date customer information and should enable the firm reliably to identify unusual and suspicious transactions and transaction patterns. Firms should ensure that they have processes in place to review flagged transactions without undue delay.

4.74. What is appropriate will depend on the nature, size and complexity of the firm's business, as well as the risk to which the firm is exposed. Firms should adjust the intensity and frequency of monitoring in line with the risk-based approach. Firms should in any case determine.

a) Which transactions they will monitor in real time, and which transactions they will monitor ex-post. As part of this, firms should determine:

i. which high-risk factors, or combination of high-risk factors, will always trigger real-time monitoring; and

ii. which transactions associated with higher ML/TF risk are monitored in real time, in particular those where the risk associated with the business relationship is already increased;

b) Whether they will monitor transactions manually or using an automated transaction monitoring system. Firms that process a high volume of transaction should consider putting in place an automated transaction monitoring system; and

c) The frequency of transaction monitoring, taking into account the requirements in these guidelines.

4.75. In addition to real time and ex-post monitoring of individual transactions, and irrespective of the level of automation used, firms should regularly perform ex-post reviews on a sample taken from all processed transactions to identify trends that could inform their risk assessments and to test and, if necessary, subsequently improve the reliability and appropriateness of their transaction monitoring system. Firms should also use the information obtained under Guidelines 1.29 to 1.30 to test and improve their transaction monitoring system.

Keeping CDD information up to date

4.76. Firms must keep CDD information up to date.[10]

4.77. When putting in place policies and procedures to keep CDD information up to date, firms should pay particular attention to the need to remain alert to, and capture, information about the customer that will help them understand whether the risk associated with the business relationship has changed. Examples of the information firms should capture include an apparent change in the source of the customer's funds, the customer's ownership structure, or behaviour that is consistently out of line with the behaviour or transaction profile the firm had expected.

4.78. A change in the customer's circumstances is likely to trigger a requirement to apply CDD measures to that customer. In those situations, firms may not need to re-apply all CDD measures, but should determine which CDD measures to apply, and the extent of the CDD measures they will apply. For example, in lower risk cases, firms may be able to draw on information obtained in the course of the business relationship to update the CDD information they hold on the customer.

Guideline 5: Record-keeping

[10] Article 14(5) of the AMLD

5.1. For the purpose of Articles 8 and 40 of Directive (EU) 2015/849, firms must keep records at least of

a) CDD information;

b) Their risk assessments; and

c) Transactions.

5.2. Firms should ensure that these records are sufficient to demonstrate to their competent authority that the measures taken are adequate in view of the ML/TF risk.

Guideline 6: Training

6.1. Firms must make their staff aware of the provisions they have put in place to comply with their AML/CFT obligations.[11]

6.2. As part of this, and in line with guidance contained in Title I, firms should take steps to ensure that staff understand

a) The business-wide risk assessment, and how it affects their daily work;

b) The firm's AML/CFT policies and procedures, and how they have to be applied; and

c) How to recognise suspicious or unusual transactions and activities, and how to proceed in such cases.

6.3. Firms should ensure that AML/CFT training is

a) Relevant to the firm and its business;

b) Tailored to staff and their specific roles;

c) Updated regularly; and

d) Effective.

Guideline 7: Reviewing effectiveness

7.1. Firms should regularly assess the effectiveness of their approach to AML/CFT and determine the frequency and intensity of such assessments on a risk-sensitive basis, taking into account the nature and size of their business and the level of ML/TF risk to which they are exposed.

[11] Article 46(1) of Directive (EU) 2015/849

7.2. Firms should consider whether an independent review of their approach may be warranted or required.[12]

[12] Article 8(4)(b) of Directive (EU) 2015/849

Title II: Sector-specific Guidelines

The sector-specific guidelines in Title II complement the general guidance in Title I of these guidelines. They should be read in conjunction with Title I.

The risk factors described in each sectoral guideline of Title II are not exhaustive. Firms should take a holistic view of the risk associated with the situation and note that isolated risk factors do not necessarily move a business relationship or occasional transaction into a higher or lower risk category.

Each sectoral guideline in Title II also sets out examples of the CDD measures firms should apply on a risk-sensitive basis in high-risk and, to the extent permitted by national legislation, low risk situations. These examples are not exhaustive and firms should decide on the most appropriate CDD measures in line with the level and type of ML/TF risk they have identified.

Guideline 8: Sectoral guideline for correspondent relationships

8.1. Guideline 8 provides guidelines on correspondent banking as defined in Article 3(8)(a) of Directive (EU) 2015/849. Firms offering other correspondent relationships as defined in Article 3(8)(b) of Directive (EU) 2015/849 should apply these guidelines as appropriate.

8.2. Firms should take into account that, in a correspondent banking relationship, the correspondent provides banking services to the respondent, either in a principal-to-principal capacity or on the respondent's customers' behalf. The correspondent does not normally have a business relationship with the respondent's customers and will not normally know their identity or the nature or purpose of the underlying transaction, unless this information is included in the payment instruction.

8.3. Firms should consider the following risk factors and measures alongside those set out in Title I of these guidelines.

Risk factors

Product, service and transaction risk factors

8.4. The following factors may contribute to increasing risk:

a) The account can be used by other respondent banks that have a direct relationship with the respondent but not with the correspondent ('nesting', or downstream clearing), which means that the correspondent is indirectly providing services to other banks that are not the respondent.

b) The account can be used by other entities within the respondent's group that have not themselves been subject to the correspondent's due diligence.

c) The service includes the opening of a payable-through account, which allows the respondent's customers to carry out transactions directly on the account of the respondent.

8.5. The following factors may contribute to reducing risk:

a) The relationship is limited to a SWIFT Risk Management Application (RMA) capability, which is designed to manage communications between financial institutions. In a SWIFT RMA relationship, the respondent, or counterparty, does not have a payment account relationship.

b) Banks are acting in a principal-to-principal capacity, rather than processing transactions on behalf of their underlying clients, for example in the case of foreign exchange services between two banks where the business is transacted

on a principal- to-principal basis between the banks and where the settlement of a transaction does not involve a payment to a third party. In those cases, the transaction is for the own account of the respondent bank.

c) The transaction relates to the selling, buying or pledging of securities on regulated markets, for example when acting as or using a custodian with direct access, usually through a local participant, to an EU or non-EU securities settlement system.

Customer risk factors

8.6. The following factors may contribute to increasing risk:

a) The respondent's AML/CFT policies and the systems and controls the respondent has in place to implement them fall short of the standards required by Directive (EU) 2015/849.

b) The respondent is not subject to adequate AML/CFT supervision.

c) The respondent, its parent or a firm belonging to the same group as the respondent has recently been the subject of regulatory enforcement for inadequate AML/CFT policies and procedures and/or breaches of AML/CFT obligations.

d) The respondent conducts significant business with sectors that are associated with higher levels of ML/TF risk; for example, the respondent conducts significant remittance business or business on behalf of certain money remitters or exchange houses, with non-residents or in a currency other than that of the country in which it is based.

e) The respondent's management or ownership includes PEPs, in particular where a PEP can exert meaningful influence over the respondent, where the PEP's reputation, integrity or suitability as a member of the management board or key function holder gives rise to concern or where the PEP is from a jurisdictions associated with higher ML/TF risk. Firms should pay particular attention to those jurisdictions where corruption is perceived to be systemic or widespread.

f) The history of the business relationship with the respondent gives rise to concern, for example because the amount of transactions is not in line with what the correspondent would expect based on its knowledge of the nature and size of the respondent.

g) The respondent´s failure to provide the information requested by the correspondent for CDD and EDD purposes, and information on the payer or the payee that is required under Regulation (EU) 2015/847. For this purpose, the correspondent should consider the quantitative and qualitative criteria set out in the Joint Guidelines JC/GL/2017/16.[13]

8.7. The following factors may contribute to reducing risk. The correspondent is satisfied that :

a) the respondent's AML/CFT controls are not less robust than those required by Directive (EU) 2015/849;

b) the respondent is part of the same group as the correspondent, is not based in a jurisdiction associated with higher ML/TF risk and complies effectively with group AML standards that are not less strict than those required by Directive (EU) 2015/849.

Country or geographical risk factors

8.8. The following factors may contribute to increasing risk:

a) The respondent is based in a jurisdiction associated with higher ML/TF risk. Firms should pay particular attention to those jurisdictions:

i. identified as high-risk third countries pursuant to Article 9(2) of Directive (EU) 2015/849;

ii. with significant levels of corruption and/or other predicate offences to money laundering;

iii. without adequate capacity of the legal and judicial system effectively to prosecute those offences;

iv. with significant levels of terrorist financing or terrorists activities; or

v. without effective AML/CFT supervision.

b) The respondent conducts significant business with customers based in a jurisdiction associated with higher ML/TF risk.

c) The respondent's parent is headquartered or is incorporated in a jurisdiction associated with higher ML/TF risk.

[13] Joint Guidelines under Article 25 of Regulation (EU) 2015/847 on the measures payment service providers should take to detect missing or incomplete information on the payer or the payee, and the procedures they should put in place to manage a transfer of funds lacking the required information issued on 22 September 2017.

8.9. The following factors may contribute to reducing risk:

a) The respondent is based in an EEA member country.

b) The respondent is based in a third country that has AML/CFT requirements not less robust than those required by Directive (EU) 2015/849 and effectively implements those requirements (although correspondents should note that this does not exempt them from applying EDD measures set out in Article 19 of Directive (EU) 2015/849).

Measures

8.10. All correspondents should carry out CDD measures set out in Article 13 of Directive (EU) 2015/849 on the respondent, who is the correspondent's customer, on a risk-sensitive basis. This means that correspondents should:

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

i. obtain information about the respondent's management and consider the relevance, for financial crime prevention purposes, of any links the respondent's management or ownership might have to PEPs or other high-risk individuals; and

ii. consider, on a risk-sensitive basis, whether obtaining information about the respondent's major business, the types of customers it attracts, and the quality of its AML systems and controls (including publicly available information about any recent regulatory or criminal sanctions for AML failings) would be appropriate. Where the respondent is a branch, subsidiary or affiliate, correspondents should also consider the status, reputation and AML controls of the parent.

b) Establish 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 of the relationship, which products and services will be supplied, and how and by whom the correspondent banking facility can be used (e.g. if it can be used by other banks through their relationship with the respondent).

c) Monitor the business relationship, including transactions, to identify changes in the respondent's risk profile and detect unusual or suspicious behaviour, including activities that are not consistent with the purpose of the services provided or that are contrary to commitments that have been concluded between the correspondent and the respondent. Where the correspondent

bank allows the respondent's customers direct access to accounts (e.g. payable-through accounts, or nested accounts), it should conduct enhanced ongoing monitoring of the business relationship. Owing to the nature of correspondent banking, post-execution monitoring is the norm.

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

8.11. Correspondents must also establish that the respondent does not permit its accounts to be used by a shell bankin line with Article 24 of Directive (EU) 2015/849. This may include asking the respondent for confirmation that it does not deal with shell banks, having sight of relevant passages in the respondent's policies and procedures, or considering publicly available information, such as legal provisions that prohibit the servicing of shell banks.

8.12. There is no requirement in Directive (EU) 2015/849 for correspondents to apply CDD measures to the respondent's individual customers.

8.13. Correspondents should take into account that CDD questionnaires provided by international organisations are not normally designed specifically to help correspondents comply with their obligations under Directive (EU) 2015/849. When considering whether to use these questionnaires, correspondents should assess whether they will be sufficient to allow them to comply with their obligations under Directive (EU) 2015/849 and should take additional steps where necessary.

Respondents based in non-EEA countries

8.14. To discharge their obligation under Article 19 of Directive (EU) 2015/849, where the correspondent relationship involves the execution of payments with a third country respondent institution, correspondents should apply specific EDD measures in addition to the CDD measures set out in Article 13 of Directive (EU) 2015/849 but can adjust those measures on a risk sensitive basis. In all other situations, firms should apply at least guideline 8.10 to 8.13.

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

8.16. Correspondents should always adequately document their CDD and EDD measures and decision-making processes.

8.17. To comply with Article 19 of Directive (EU) 2015/849, the risk-sensitive measures firms take should enable them to:

a) Gather sufficient information about a respondent institution to understand fully the nature of the respondent's business, in order to establish the extent to which the respondent's business exposes the correspondent to higher money-laundering risk. This should include taking steps to understand and risk-assess the nature of respondent's customer base, if necessary by asking the respondent about its customers, and the type of activities that the respondent will transact through the correspondent account.

b) Determine from publicly available information the reputation of the institution and the quality of supervision. This means that the correspondent should assess the extent to which the correspondent can take comfort from the fact that the respondent is adequately supervised for compliance with its AML obligations. A number of publicly available resources, for example FATF or FSAP assessments, which contain sections on effective supervision, may help correspondents establish this.

c) Assess the respondent institution's AML/CFT controls. This implies that the correspondent should carry out a qualitative assessment of the respondent's AML/CFT control framework, not just obtain a copy of the respondent's AML policies and procedures. This assessment should be documented appropriately. In line with the risk-based approach, where the risk is especially high and in particular where the volume of correspondent banking transactions is substantive, the correspondent should consider on-site visits and/or sample testing to be satisfied that the respondent's AML policies and procedures are implemented effectively.

d) Obtain approval from senior management, as defined in Article 3(12) of Directive (EU) 2015/849 before establishing new correspondent relationships and where material new risks emerge, such as because the country in which the respondent is based is designated as high risk under provisions in Article 9 of Directive (EU) 2015/849.. The approving senior manager should not be the officer sponsoring the relationship and the higher the risk associated with the relationship, the more senior the approving senior manager should be. Correspondents should keep senior management informed of high-risk correspondent banking relationships and the steps the correspondent takes to manage that risk effectively.

e) Document the responsibilities of each institution. If not already specified in its standard agreement, the correspondents should conclude a written agreement including at least the following:

i. the products and services provided to the respondent,

ii. how and by whom the correspondent banking facility can be used (e.g. if it can be used by other banks through their relationship with the respondent), what the respondent's AML/CFT responsibilities are;

iii. how the correspondent will monitor the relationship to ascertain the respondent complies with its responsibilities under this agreement (for example through ex post transaction monitoring);

iv. the information that should be supplied by the respondent at the correspondent's request (in particular for the purpose of monitoring the correspondent relationship) and a reasonable deadline by which the information should be provided (taking into account the complexity of the payment chain or the correspondent chain) .

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

Respondents based in EEA countries

8.18. Where the respondent is based in an EEA country, Article 19 of Directive (EU) 2015/849 does not apply. The correspondent is, however, still obliged to apply risk-sensitive CDD measures pursuant to Article 13 of Directive (EU) 2015/849.

8.19. Where the risk associated with a respondent based in an EEA Member State is increased, correspondents must apply EDD measures in line with Article 18 of Directive (EU) 2015/849. In that case, correspondents should consider applying at least some of the EDD measures described in Article 19 of Directive (EU) 2015/849, in particular Article 19(a) and (b).

Respondents established in high-risk third countries, and correspondent relationships involving high-risk third countries

8.20. Correspondents should determine which of their relationships involve high-risk third countries, identified pursuant to Article 9(2) of Directive (EU) 2015/849.

8.21. Correspondents should also, as part of their standard CDD measures, determine the likelihood of the respondent initiating transactions involving high-risk third countries, including where a significant proportion of the respondent's own customers maintain relevant professional or personal links to high-risk third countries.

8.22. To discharge their obligation under Article 18a, firms should ensure that they also apply Article 13 and 19 of Directive (EU) 2015/849.

8.23. Unless the correspondent has assessed ML/TF risk arising from the relationship with the respondent as particularly high correspondents should be able to comply with the requirements in Article 18a(1) by applying Article 13 and 19 of Directive (EU) 2015/849.

8.24. To discharge their obligation under Article 18a(1)(c) of Directive (EU)2015/849, correspondents should apply guideline 8.17(c) and take care to assess the adequacy of the respondent's policies and procedures to establish their customers' source of funds and source of wealth, carry out onsite visits or sample checks, or ask the respondent to provide evidence of the legitimate origin of a particular customer's source of wealth or source of funds, as required.

8.25. Where Members States require firms to apply additional measures in line with article 18a)(2)correspondents should apply one or more of the following:

a) Increasing the frequency of reviews of CDD information held on the respondent, and the risk assessment of that respondent;

b) Requiring a more in-depth assessment of the respondent´s AML/CFT controls. In these higher risk situations, correspondents should consider reviewing the independent audit report of the respondent's AML/CFT controls, interviewing the compliance officers, commissioning a third party review or conducting an onsite visit.

c) Requiring increased and more intrusive monitoring. Real-time monitoring of transactions is one of the EDD measures banks should consider in situations where the ML/TF risk is particularly increased. As part of this, correspondents should consider maintaining an ongoing dialogue with the respondent to develop a better understanding of the risks associated with the correspondent relationship and facilitate the rapid exchange of meaningful information, if necessary.

d) Requiring increased monitoring on transfers of funds to ensure detection of missing or incomplete information on the payer and or the payee under Regulation (EU) 2015/847 and in line with the Joint Guidelines JC/GL/2017/16.[14]

e) Limiting business relationships or transactions involving high-risk third countries in terms of nature, volume or means of payment, after a thorough assessment of the residual risk posed by the correspondent relationship.

[14] Joint Guidelines under Article 25 of Regulation (EU) 2015/847 on the measures payment service providers should take to detect missing or incomplete information on the payer or the payee, and the procedures they should put in place to manage a transfer of funds lacking the required information issued on 22 September 2017 (JC/GL/2017/16).

Guideline 9: Sectoral guideline for retail banks

9.1. For the purpose of these guidelines, retail banking means the provision of banking services to natural persons and small and medium-sized enterprises. Examples of retail banking products and services include current accounts, mortgages, savings accounts, consumer and term loans, and credit lines.

9.2. Owing to the nature of the products and services offered, the relative ease of access and the often large volume of transactions and business relationships, retail banking is vulnerable to terrorist financing and to all stages of the money laundering process. At the same time, the volume of business relationships and transactions associated with retail banking can make identifying ML/TF risk associated with individual relationships and spotting suspicious transactions particularly challenging.

9.3. Banks should consider the following risk factors and measures alongside those set out in Title I of these guidelines. Banks that provide payment initiation services or account information services should also refer to the sectoral guideline 18.

Risk factors

Product, service and transaction risk factors

9.4. The following factors may contribute to increasing risk:

a) the product's features favour anonymity;

b) the product allows payments from third parties that are neither associated with the product nor identified upfront, where such payments would not be expected, for example for mortgages or loans;

c) the product places no restrictions on turnover, cross-border transactions or similar product features;

d) new products and new business practices, including new delivery mechanisms, and the use of new or developing technologies for both new and existing products where these are not yet well understood;

e) lending (including mortgages) secured against the value of assets in other jurisdictions, particularly countries where it is difficult to ascertain whether the customer has legitimate title to the collateral, or where the identities of parties guaranteeing the loan are hard to verify;

f) an unusually high volume or large value of transactions.

9.5. The following factors may contribute to reducing risk:

a) The product has limited functionality, for example in the case of:

i. a fixed term savings product with low savings thresholds;

ii. a product where the benefits cannot be realised for the benefit of a third party;

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

iv. a low-value loan facility, including one that is conditional on the purchase of a specific consumer good or service; or

v. a low-value product, including a lease, where the legal and beneficial title to the asset is not transferred to the customer until the contractual relationship is terminated or is never passed at all.

b) 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.

c) Transactions must be carried out through an account in the customer's name at a credit or financial institution that is subject to AML/CFT requirements that are not less robust than those required by Directive (EU) 2015/849.

d) There is no overpayment facility.

Customer risk factors

9.6. The following factors may contribute to increasing risk:

a) The nature of the customer, for example:

i. The customer is a cash-intensive undertaking.

ii. The customer is an undertaking associated with higher levels of money laundering risk, for example certain money remitters and gambling businesses.

iii. The customer is an undertaking associated with a higher corruption risk, for example operating in the extractive industries or the arms trade.

iv. The customer is a non-profit organisation that supports jurisdictions associated with an increased TF risk

v. The customer is a new undertaking without an adequate business profile or track record.

vi. The customer is a non-resident. Banks should note that Article 16 of Directive 2014/92/EU creates a right for consumers who are legally resident in the European Union to obtain a basic bank account, although the right to open and use a basic payment account applies only to the extent that banks can comply with their AML/CFT obligations and does not exempt banks from their obligation to identify and assess ML/TF risk, including the risk associated with the customer not being a resident of the Member State in which the bank is based.[15]

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

b) The customer's behaviour, for example:

i. The customer is reluctant to provide CDD information or appears deliberately to avoid face-to-face contact.

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

iii. The customer's behaviour or transaction volume is not in line with that expected from the category of customer to which they belong, or is unexpected based on the information the customer provided at account opening.

iv. The customer's behaviour is unusual, for example the customer unexpectedly and without reasonable explanation accelerates an agreed repayment schedule, by means either of lump sum repayments or early termination; deposits or demands payout of high-value bank notes without apparent reason; increases activity after a period of dormancy; or makes transactions that appear to have no economic rationale.

9.7. The following factor may contribute to reducing risk: ¨

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

Country or geographical risk factors

9.8. The following factors may contribute to increasing risk: ¸

[15] See the EBA's 'Opinion on the application of customer due diligence measures to customers who are asylum seekers from higher-risk third countries or territories': http://www.eba.europa.eu/documents/10180/1359456/EBA-Op-2016-07+%28Opinion+on+Customer+Due+Diligence+on+Asylum+Seekers%29.pdf

a) The customer's funds are derived from personal or business links to jurisdictions associated with higher ML/TF risk.

b) The payee is located in a jurisdiction associated with higher ML/TF risk. Firms should pay particular attention to jurisdictions known to provide funding or support for terrorist activities or where groups committing terrorist offences are known to be operating, and jurisdictions subject to financial sanctions, embargoes or measures that are related to terrorism, financing of terrorism or proliferation.

9.9. The following factor may contribute to reducing risk:

a) Countries associated with the transaction have an AML/CFT regime that is not less robust than that required under Directive (EU) 2015/849 and are associated with low levels of predicate offences.

Distribution channel risk factors

9.10. The following factors may contribute to increasing risk:

a) non-face-to-face business relationships, where no adequate additional safeguards – for example electronic signatures, electronic identification means in accordance with Regulation EU (No) 910/2014 and anti-impersonation fraud checks – are in place;

b) reliance on a third party's CDD measures in situations where the bank does not have a long-standing relationship with the referring third party;

c) new delivery channels that have not been tested yet.

9.11. The following factor may contribute to reducing risk:

a) The product is available only to customers who meet specific eligibility criteria set out by national public authorities, as in the case of state benefit recipients or specific savings products for children registered in a particular Member State.

Measures

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

Enhanced customer due diligence

9.13. Where the risk associated with a business relationship or occasional transaction is increased, banks must apply EDD measures pursuant to Article 18 of Directive (EU) 2015/849. These may include:

a) Verifying the customer's and the beneficial owner's identity on the basis of more than one reliable and independent source.

b) Identifying, and verifying the identity of, other shareholders who are not the customer's beneficial owner or any natural persons who have authority to operate an account or give instructions concerning the transfer of funds or the transfer of securities.

c) Obtaining more information about the customer and the nature and purpose of the business relationship to build a more complete customer profile, for example by carrying out open source or adverse media searches or commissioning a third party intelligence report. Examples of the type of information banks may seek include:

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

ii. the source of the customer's wealth and the source of the customer's funds that are involved in the business relationship, to be reasonably satisfied that these are legitimate;

iii. the purpose of the transaction, including, where appropriate, the destination of the customer's funds;

iv. information on any associations the customer might have with other jurisdictions (headquarters, operating facilities, branches, etc.) and the individuals who may influence its operations; or

v. where the customer is based in another country, why they seek retail banking services outside their home jurisdiction.

d) Increasing the frequency of transaction monitoring.

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

9.14. In respect of business relationships or transactions involving high-risk third countries, banks should follow the guidance in Title I.

Simplified customer due diligence

9.15. In low-risk situations, and to the extent permitted by national legislation, banks may apply SDD measures, which may include:

a) for customers that are subject to a statutory licensing and regulatory regime, verifying identity based on evidence of the customer being subject to that regime, for example through a search of the regulator's public register;

b) verifying the customer's and, where applicable, the beneficial owner's identities during the establishment of the business relationship in accordance with Article 14(2) of Directive (EU) 2015/849;

c) assuming that a payment drawn on an account in the sole or joint name of the customer at a regulated credit or financial institution in an EEA country satisfies the requirements stipulated by Article 13(1)(a) and (b) of Directive (EU) 2015/849;

d) accepting alternative forms of identity that meet the independent and reliable source criterion in Article 13(1)(a) of Directive (EU) 2015/849, such as a letter from a government agency or other reliable public body to the customer, where there are reasonable grounds for the customer not to be able to provide standard evidence of identity and provided that there are no grounds for suspicion;

e) updating CDD information only in case of specific trigger events, such as the customer requesting a new or higher risk product, or changes in the customer's behaviour or transaction profile that suggest that the risk associated with the relationship is no longer low.

Pooled accounts

9.16. Where a bank's customer opens a 'pooled account' in order to administer funds that belong to the customer's own clients, the bank should apply full CDD measures, including treating the customer's clients as the beneficial owners of funds held in the pooled account and verifying their identities.

9.17. Where there are indications that the risk associated with the business relationship is high, banks must apply EDD measures set out in Article 18 of Directive (EU) 2015/849 as appropriate.

9.18. However, to the extent permitted by national legislation, where the risk associated with the business relationship is low and subject to the conditions set out below, a bank may apply SDD measures provided that:

a) The customer is a firm that is subject to AML/CFT obligations in an EEA state or a third country with an AML/CFT regime that is not less robust than that required by Directive (EU) 2015/849, and is supervised effectively for compliance with these requirements.

b) The customer is not a firm but another obliged entity that is subject to AML/CFT obligations in an EEA state and is supervised effectively for compliance with these requirements.

c) The ML/TF risk associated with the business relationship is low, based on the bank's assessment of its customer's business, the types of clients the customer's business serves and the jurisdictions the customer's business is exposed to, among other considerations;

d) the bank is satisfied that the customer applies robust and risk-sensitive CDD measures to its own clients and its clients' beneficial owners (it may be appropriate for the bank to take risk-sensitive measures to assess the adequacy of its customer's CDD policies and procedures, for example by liaising directly with the customer); and

e) the bank has taken risk-sensitive steps to be satisfied that the customer will provide CDD information and documents on its underlying clients that are the beneficial owners of funds held in the pooled account immediately upon request, for example by including relevant provisions in a contract with the customer or by sample-testing the customer's ability to provide CDD information upon request.

9.19. Where the conditions for the application of SDD to pooled accounts are met, SDD measures may consist of the bank:

a) identifying and verifying the identity of the customer, including the customer's beneficial owners (but not the customer's underlying clients);

b) assessing the purpose and intended nature of the business relationship; and

c) conducting ongoing monitoring of the business relationship.

Customers that offer services related to virtual currencies

9.20. Firms should take into account the fact that apart from providers engaged in exchange services between virtual currency and fiat currencies and Custodian Wallet Providers which are obliged entities under Directive (EU) 2015/849, the issuing or holding of virtual currencies as defined in point (18) of Article 3 of Directive (EU) 2015/849 remains largely unregulated

in the EU and this increases the ML/TF risks. Firms may wish to refer to the EBA's report on crypto assets of January 2019.

9.21. When entering into a business relationship with customers that provide services related to virtual currencies, firms should, as part of their ML/TF risk assessment of the customer, consider the ML/TF risk associated with virtual currencies.

9.22. Firms should consider among others the following as virtual currency businesses:

a) Operating as a virtual currency trading platform that effects exchanges between fiat currency and virtual currency;

b) Operating as a virtual currency trading platform that effects exchanges between virtual currencies;

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

d) Providing custodian wallet services;

e) Arranging, advising or benefiting from 'initial coin offerings' (ICOs).

9.23. To ensure that the level of ML/TF risk associated with such customers is mitigated, banks should not apply simplified due diligence measures. At a minimum as part of their CDD measures, firms should:

a) Enter into dialogue with the customer to understand the nature of the business and the ML/TF risks it poses;

b) In addition to verifying the identity of the customer's beneficial owners, carry out due diligence on senior management to the extent that they are different, including consideration of any adverse information ;

c) Understand the extent to which these customers apply their own customer due diligence measures to their clients either under a legal obligation or on a voluntary basis.

d) Establish whether the customer is registered or licensed in an EEA Member State, or in a third country, and take a view on the adequacy of that third country's AML/CFT regime;

e) Finding out whether businesses using ICOs in the form of virtual currencies to raise money are legitimate and, where applicable, regulated.

9.24. Where the risk associated with such customers is increased, banks should apply EDD measures in line with Title I.

Guideline 10: Sectoral guideline for electronic money issuers

10.1. Guideline 10 provides guidelines for electronic money issuers (e-money issuers) as defined in Article 2(3) of Directive 2009/110/EC. The level of ML/TF risk associated with electronic money as defined in Article 2(2) of Directive 2009/110/EC (e-money) depends primarily on the features of individual e-money products and the degree to which e-money issuers use other persons to distribute and redeem e-money on their behalf pursuant to Article 3(4) of Directive 2009/110/EC.

10.2. Firms that issue e-money should consider the following risk factors and measures alongside those set out in Title I of these guidelines. Firms whose authorisation includes the provision of business activities as payment initiation services and account information services s should also refer to the sectoral guideline 18. The sectoral guideline 11 for money remitters may also be relevant in this context.

Risk factors

Product risk factors

10.3. E-money issuers should consider the ML/TF risk related to:

a) thresholds;

b) the funding method; and

c) utility and negotiability.

10.4. The following factors may contribute to increasing risk:

a) Thresholds: the product allows

i. high-value or unlimited-value payments, loading or redemption, including cash withdrawal;

ii. high number of payments, loading or redemption, including cash withdrawal;

iii. high or unlimited amount of funds to be stored on the e-money product/account.

b) Funding method: the product can be

i. loaded anonymously, for example with cash, anonymous e-money or e-money products that benefit from the exemption in Article 12 of Directive (EU) 2015/849;

ii. funded with payments from unidentified third parties;

iii. funded with other e-money products.

c) Utility and negotiability: the product

i. allows person-to-person transfers;

ii. is accepted as a means of payment by a large number of merchants or points of sale;

iii. is designed specifically to be accepted as a means of payment by merchants dealing in goods and services associated with a high risk of financial crime, for example online gambling;

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

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

vi. allows high-value cash withdrawals.

10.5. The following factors may contribute to reducing risk:

a) Thresholds: the product

i. sets low-value limits on payments, loading or redemption, including cash withdrawal (although firms should note that a low threshold alone may not be enough to reduce TF risk);

ii. limits number of payments, loading or redemption, including cash withdrawal in a given period;

iii. limits the amount of funds that can be stored on the e-money product/account at any one time.

b) Funding: the product

i. requires that the funds for purchase or reloading are verifiably drawn from an account held in the customer's sole or joint name at an EEA credit or financial institution;

c) Utility and negotiability: the product

i. does not allow or strictly limits cash withdrawal;

ii. can be used only domestically;

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

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

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

Customer risk factors

10.6. The following factors may contribute to increasing risk:

a) The customer purchases several e-money products from the same issuer, frequently reloads the product or make several cash withdrawals in a short period of time and without an economic rationale; where distributors (or agents acting as distributors) are obliged entities themselves, this also applies to e-money products from different issuers purchased from the same distributor.

b) The customer's transactions are always just below any value/transaction limits.

c) The product appears to be used by several people whose identity is not known to the issuer (e.g. the product is used from several IP addresses at the same time).

d) There are frequent changes in the customer's identification data, such as home address or IP address, or linked bank accounts.

e) The product is not used for the purpose it was designed for, for example it is used overseas when it was designed as a shopping centre gift card.

10.7. The following factor may contribute to reducing risk:

a) The product is available only to certain categories of customers, for example social benefit recipients or employees of a company that issues them to cover corporate expenses.

Distribution channel risk factors

10.8. The following factors may contribute to increasing risk:

a) Online and non-face-to-face distribution without adequate safeguards, such as electronic signatures, electronic identification means meeting the criteria set out in Regulation (EU) No 910/2014 and anti-impersonation fraud measures.

b) Distribution through intermediaries that are not themselves obliged entities under Directive (EU) 2015/849 or national legislation where applicable, where the e-money issuer:

i. relies on the intermediary to carry out some of the AML/CFT obligations of the e-money issuer;

ii. has not satisfied itself that the intermediary has in place adequate AML/CFT systems and controls; and

iii. segmentation of services, that is, the provision of e-money services by several operationally independent service providers without due oversight and coordination.

10.9. Firms should, prior to signing a distribution agreement with a merchant, understand the nature and purpose of the merchant's business to satisfy themselves that the goods and services provided are legitimate and to assess the ML/TF risk associated with the merchant's business. In case of an online merchant, firms should also take steps to understand the type of customers this merchant attracts, and establish the expected volume and size of transactions in order to spot suspicious or unusual transactions

Country or geographical risk factors

10.10. The following factors may contribute to increasing risk:

a) The payee is located in a jurisdiction associated with higher ML/TF risk and/or the product has been issued or receives funds from sources in such a jurisdiction. Firms should pay particular attention to jurisdictions known to provide funding or support for terrorist activities or where groups committing terrorist offences are known to be operating, and jurisdictions subject to financial sanctions, embargoes or measures that are related to terrorism, financing of terrorism or proliferation.

Measures

Customer Due Diligence measures

10.11. Firms should apply CDD measures to:

a) The owner of the electronic money account or product; and

b) Additional card holders. Where products are linked to multiple cards, firms should establish whether they have entered into one or more business relationships, and whether additional card holders could be beneficial owners.

10.12. National legislation may provide for an exemption from identification and verification of the customer's and beneficial owners' identities and assessment of the nature and purpose of the business relationship for certain E-money products in accordance with Article 12 of Directive (EU) 2015/849.

10.13. Firms should note that the exemption under Article 12 of Directive (EU) 2015/849 does not extend to the obligation to conduct ongoing monitoring of transactions and the business relationship, nor does it exempt them from the obligation to identify and report suspicious transactions; this means that firms should ensure that they obtain sufficient information about their customers, or the types of customers their product will target, to be able to carry out meaningful ongoing monitoring of the business relationship.

10.14. Examples of the types of monitoring systems firms should put in place include:

a) transaction monitoring systems that detect anomalies or suspicious patterns of behaviour, including the unexpected use of the product in a way for which it was not designed; the firm may be able to disable the product either manually or through on- chip controls until it has been able to satisfy itself that there are no grounds for suspicion;

b) systems that identify discrepancies between submitted and detected information, for example, between submitted country of origin information and the electronically detected IP address;

c) systems that compare data submitted with data held on other business relationships and that can identify patterns such as the same funding instrument or the same contact details;

d) systems that identify whether the product is used with merchants dealing in goods and services that are associated with a high risk of financial crime;

e) systems that link e-money products to devices or IP addresses for web-based transactions.

Enhanced customer due diligence

10.15. To comply with Article 18a in respect of relationships or transactions involving high-risk third countries, e-money issuers should apply the EDD measures set out in this regard in Title I.

10.16. Examples of EDD measures firms should apply in all other high-risk situations include:

a) obtaining additional customer information during identification, such as the source of funds;

b) applying additional verification measures from a wider variety of reliable and independent sources (e.g. checking against online databases) in order to verify the customer's or beneficial owner's identity;

c) obtaining additional information about the intended nature of the business relationship, for example by asking customers about their business or the jurisdictions to which they intend to transfer E-money;

d) obtaining information about the merchant/payee, in particular where the E-money issuer has grounds to suspect that its products are being used to purchase illicit or age-restricted goods;

e) applying identity fraud checks to ensure that the customer is who they claim to be;

f) applying enhanced monitoring to the customer relationship and individual transactions;

g) establishing the source and/or the destination of funds.

Simplified customer due diligence

10.17. To the extent permitted by national legislation, firms may consider applying SDD to low-risk e-money products that do not benefit from the exemption provided by Article 12 of Directive (EU) 2015/849.

10.18. To the extent permitted by national legislation, examples of SDD measures firms may apply in low-risk situations include:

a) postponing the verification of the customer's or beneficial owner's identity to a certain later date after the establishment of the relationship or until a certain (low) monetary threshold is exceeded (whichever occurs first). The monetary threshold should not exceed EUR 150 where the product is not reloadable or can be used in other jurisdictions or for cross-border transactions);

b) verifying the customer's identity on the basis of a payment drawn on an account in the sole or joint name of the customer or an account over which the customer can be shown to have control with an EEA-regulated credit or financial institution;

c) verifying identity on the basis of fewer sources;

d) verifying identity on the basis of less reliable sources;

e) using alternative methods to verify identity;

f) assuming the nature and intended purpose of the business relationship where this is obvious, for example in the case of certain gift cards that do not fall under the closed loop/closed network exemption;

g) reducing the intensity of monitoring as long as a certain monetary threshold is not reached. As ongoing monitoring is an important means of obtaining more information on customer risk factors (see above) during the course of a customer relationship, that threshold for both individual transactions and transactions that appear to be linked over the course of 12 months should be set at a level that the firm has assessed as presenting a low risk for both terrorist financing and money laundering purposes.

Guideline 11: Sectoral guideline for money remitters

11.1. Money remitters are payment institutions or e-money institutions or credit institutions that have been authorised in line with Directive (EU) 2015/2366 to provide and execute payment services throughout the EU. The businesses in this sector are diverse and range from individual businesses to complex chain operators.

11.2. Many money remitters use agents to provide payment services on their behalf. Agents often provide payment services as an ancillary component to their main business and they may not themselves be obliged entities under applicable AML/CFT legislation; accordingly, their AML/CFT expertise may be limited.

11.3. The nature of the service provided can expose money remitters to ML/TF risk. This is due to the simplicity and speed of transactions, their worldwide reach and their often cash-based character. Furthermore, the nature of this payment service means that money remitters often carry out occasional transactions rather than establishing a business relationship with their customers, which means that their understanding of the ML/TF risk associated with the customer may be limited.

11.4. Money remitters should consider the following risk factors and measures alongside those set out in Title I of these guidelines. Firms whose authorisation includes the provision of business activities as Payment Initiation Services and Account Initiation Services should also refer to the sectoral guideline 18.

Risk factors

Product, service and transaction risk factors

11.5. The following factors may contribute to increasing risk:

a) the product allows high-value or unlimited-value transactions;

b) the product or service has a global reach;

c) the transaction is cash-based or funded with anonymous electronic money, including electronic money benefiting from the exemption under Article 12 of Directive (EU) 2015/849;

d) transfers are made from one or more payers in different countries to a local payee.

11.6. The following factor may contribute to reducing risk:

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

Customer risk factors

11.7. The following factors may contribute to increasing risk:

a) The customer's business activity:

i. The customer owns or operates a business that handles large amounts of cash.

ii. The customer's business has a complicated ownership structure.

iii. The customer´s activity could be associated with TF because he is publicly known to have extremism sympathies or are known to be linked to an organised crime group.

b) The customer's behaviour:

i. The customer's needs may be better serviced elsewhere, for example because the money remitter is not local to the customer or the customer's business.

ii. The customer appears to be acting for someone else, for example others watch over the customer or are visible outside the place where the transaction is made, or the customer reads instructions from a note.

iii. The customer's behaviour makes no apparent economic sense, for example the customer accepts a poor exchange rate or high charges unquestioningly, requests a transaction in a currency that is not official tender or commonly used in the jurisdiction where the customer and/or recipient is located or requests or provides large amounts of currency in either low or high denominations.

iv. The customer's transactions are always just below applicable thresholds, including the CDD threshold for occasional transactions in Article 11(b) of Directive (EU) 2015/849 and the EUR 1 000 threshold specified in Article 5(2) of Regulation (EU) 2015/847.[16] Firms should note that the threshold in Article 5(2) of Regulation (EU) 2015/847 applies only to transactions that are not funded by cash or anonymous electronic money.

v. The customer's use of the service is unusual, for example they send or receive money to or from themselves or send funds on immediately after receiving them.

vi. The customer appears to know little or is reluctant to provide information about the payee.

[16] Regulation (EU) 2015/847 of the European Parliament and of the Council of 20 May 2015 on information accompanying transfers of funds and repealing Regulation (EC) No 1781/2006.

vii. Several of the firm's customers transfer funds to the same payee or appear to have the same identification information, for example address or telephone number.

viii. An incoming transaction is not accompanied by the required information on the payer or payee.

ix. The amount sent or received is at odds with the customer's income (if known).

x. The increase of volume or number of transactions is not related to a usual pattern like salary remittance or cultural celebration.

xi. The customer provides inconsistent biographical data or identification documents containing inconsistent information.

11.8. The following factors may contribute to reducing risk:

a) The customer is a long-standing customer of the firm whose past behaviour has not given rise to suspicion and there are no indications that the ML/TF risk might be increased

b) The amount transferred is low; however, firms should note that low amounts alone will not be enough to discount TF risk.

Distribution channel risk factors

11.9. The following factors may contribute to increasing risk:

a) There are no restrictions on the funding instrument, for example in the case of cash or payments from E-money products that benefit from the exemption in Article 12 of Directive (EU) 2015/849, wire transfers or cheques.

b) The distribution channel used provides a degree of anonymity.

c) The service is provided entirely online without adequate safeguards.

d) The money remittance service is provided through agents that:

i. represent more than one principal;

ii. have unusual turnover patterns compared with other agents in similar locations, for example unusually high or low transaction sizes, unusually large cash transactions or a high number of transactions that fall just under the CDD threshold, or undertake business outside normal business hours;

iii. undertake a large proportion of business with payers or payees from jurisdictions associated with higher ML/TF risk;

iv. appear to be unsure about, or inconsistent in, the application of group-wide AML/CFT policies; or

v. are not from the financial sector and conduct another business as their main business.

e) The money remittance service is provided through a large network of agents in different jurisdictions.

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

11.10. The following factors may contribute to reducing risk:

a) Agents are themselves regulated financial institutions.

b) The service can be funded only by transfers from an account held in the customer's name at an EEA credit or financial institution or an account over which the customer can be shown to have control.

Country or geographical risk factors

11.11. The following factors may contribute to increasing risk:

a) The payer or the payee is located , or the transaction is executed from an IP address, in a jurisdiction associated with higher ML/TF risk. Firms should pay particular attention to jurisdictions known to provide funding or support for terrorist activities or where groups committing terrorist offences are known to be operating, and jurisdictions subject to financial sanctions, embargoes or measures that are related to terrorism, financing of terrorism or proliferation.

b) The payee is resident in a jurisdiction that has no, or a less developed, formal banking sector, which means that informal money remittance services, such as hawala, may be used at point of payment.

c) The firm's counterparty is located in a third country [associated with higher ML/TF risk]

d) The payer or the payee is located in a high-risk third country.

Measures

11.12. Since many money remitters' business is primarily transaction-based, firms should consider which monitoring systems and controls they put in place to ensure that they detect money-laundering and terrorist financing attempts even where the CDD information they hold on the customer is basic or missing because no business relationship has been established. When analysing appropriate monitoring systems, money remitters should ensure that are aligned with the size and complexity of the business and their transaction volume.

11.13. Firms should in any case put in place:

a) systems to identify linked transactions, including those that might amount to a business relationship according to their policies and procedures, such as systems to identify series of transactions bellow EUR 1 000 which have the same payer and payee and an element of duration;

b) systems to identify whether transactions from different customers are destined for the same payee;

c) systems to permit as far as possible the establishment of the source of funds and the destination of funds;

d) systems that allow the full traceability of both transactions and the number of operators included in the payment chain;

e) systems that identify whether a transfer is made to, or received from, a high risk third country; and

f) systems to ensure that throughout the payment chain only those duly authorised to provide money remittance services can intervene.

11.14. Where the risk associated with an occasional transaction or business relationship is increased, firms should apply EDD in line with Title I, including, where appropriate, increased transaction monitoring (e.g. increased frequency or lower thresholds). Conversely, where the risk associated with an occasional transaction or business relationship is low and to the extent permitted by national legislation, firms may be able to apply SDD measures in line with Title I.

11.15. To comply with Article 18a of Directive (EU) 2015/849 in respect of relationships or transactions involving high-risk third countries, money remitter should apply the EDD measures set out in this regard in Title I.

Use of agents

11.16. Money remitters using agents to provide payment services should know who their agents as set out in Article 19 of Directive (EU) 2015/2366 are. As part of this, money remitters should establish and maintain appropriate and risk- sensitive policies and procedures to counter the risk that their agents may engage in, or be used for, ML/TF, including by:

a) Identifying the person who owns or controls the agent where the agent is a legal person, to be satisfied that the ML/TF risk to which the money remitter is exposed as a result of its use of the agent is not increased.

b) Obtaining evidence, in line with the requirements of Article 19(1)(c) of Directive (EU) 2015/2366, that the directors and other persons responsible for the management of the agent are fit and proper persons, including by considering their honesty, integrity and reputation. Any enquiry the money remitter makes should be proportionate to the nature, complexity and scale of the ML/TF risk inherent in the payment services provided by the agent and could be based on the money remitter's CDD procedures.

c) Taking reasonable measures to satisfy themselves that the agent's AML/CFT internal controls are appropriate and remain appropriate throughout the agency relationship, for example by monitoring a sample of the agent's transactions or reviewing the agent's controls on site. Where an agent's internal AML/CFT controls differ from the money remitter's, for example because the agent represents more than one principal or because the agent is itself an obliged entity under applicable AML/CFT legislation, the money remitter should assess and manage the risk that these differences might affect its own, and the agent's, AML/CFT compliance.

d) Providing AML/CFT training to agents to ensure that agents have an adequate understanding of relevant ML/TF risks and the quality of the AML/CFT controls the money remitter expects.

Guideline 12: Sectoral guideline for wealth management

12.1. Wealth management is the provision of banking and other financial services to high-net-worth individuals and their families or businesses. It is also known as private banking. Clients of wealth management firms can expect dedicated relationship management staff to provide tailored services covering, for example, banking (e.g. current accounts, mortgages and foreign exchange), investment management and advice, fiduciary services, safe custody, insurance, family office services, tax and estate planning and associated facilities, including legal support.

12.2. Many of the features typically associated with wealth management, such as wealthy and influential clients; very high-value transactions and portfolios; complex products and services, including tailored investment products; and an expectation of confidentiality and discretion are indicative of a higher risk for money laundering relative to those typically present in retail banking. Wealth management firms' services may be particularly vulnerable to abuse by clients who wish to conceal the origins of their funds or, for example, evade tax in their home jurisdiction.

12.3. Firms in this sector should consider the following risk factors and measures alongside those set out in Title I of these guidelines. The sectoral guidelines 9, 14 and 17 in Title I, may also be relevant in this context.

Risk factors

Product, service and transaction risk factors

12.4. The following factors may contribute to increasing risk:

a) customers requesting large amounts of cash or other physical stores of value such as precious metals;

b) very high-value transactions;

c) financial arrangements involving jurisdictions associated with higher ML/TF risk (firms should pay particular attention to countries that have a culture of banking secrecy or that do not comply with international tax transparency standards);

d) lending (including mortgages) secured against the value of assets in other jurisdictions, particularly countries where it is difficult to ascertain whether the customer has legitimate title to the collateral, or where the identities of parties guaranteeing the loan are hard to verify;

e) the use of complex business structures such as trusts and private investment vehicles, particularly where the identity of the ultimate beneficial owner may be unclear;

f) business taking place across multiple countries, particularly where it involves multiple providers of financial services;

g) cross-border arrangements where assets are deposited or managed in another financial institution, either of the same financial group or outside the group, particularly where the other financial institution is based in a jurisdiction associated with higher ML/TF risk. Firms should pay particular attention to jurisdictions with higher levels of predicate offences, a weak AML/CFT regime or weak tax transparency standards.

Customer risk factors

12.5. The following factors may contribute to increasing risk:

a) Customers with income and/or wealth from high-risk sectors such as arms, the extractive industries, construction, gambling or private military contractors.

b) Customers about whom credible allegations of wrongdoing have been made.

c) Customers who expect unusually high levels of confidentiality or discretion.

d) Customers whose spending or transactional behaviour makes it difficult to establish 'normal', or expected patterns of behaviour.

e) Very wealthy and influential clients, including customers with a high public profile, non-resident customers and PEPs. Where a customer or a customer's beneficial owner is a PEP, firms must always apply EDD in line with Articles 18 to 22 of Directive (EU) 2015/849.

f) The customer requests that the firm facilitates the customer being provided with a product or service by a third party without a clear business or economic rationale.

Country or geographical risk factors

12.6. The following factors may contribute to increasing risk:

a) Business is conducted in countries that have a culture of banking secrecy or do not comply with international tax transparency standards.

b) The customer lives in, or their funds derive from activity in, a jurisdiction associated with higher ML/TF risk.

Measures

12.7. The staff member managing a wealth management firm's relationship with a customer (the relationship manager) typically plays a key role in assessing risk. The relationship manager's close contact with the customer will facilitate the collection of information that allows a fuller picture of the purpose and nature of the customer's business to be formed (e.g. an understanding of the client's source of wealth, the destination of funds, why complex or unusual arrangements may nonetheless be genuine and legitimate, or why extra security may be appropriate). This close contact may, however, also lead to conflicts of interest if the relationship manager becomes too close to the customer, to the detriment of the firm's efforts to manage the risk of financial crime. Consequently, independent oversight of risk assessment will also be appropriate, provided by, for example, the compliance department and senior management.

Enhanced customer due diligence

12.8. To comply with Article 18a in respect of relationships or transactions involving high-risk third countries, firms should apply the EDD measures set out in this regard in Title I.

a) Obtaining and verifying more information about clients than in standard risk situations and reviewing and updating this information both on a regular basis and when prompted by material changes to a client's profile. Firms should perform reviews on a risk-sensitive basis, reviewing higher risk clients at least annually but more frequently if risk dictates. These procedures may include those for recording any visits to clients' premises, whether at their home or business, including any changes to client profile or other information that may affect risk assessment that these visits prompt.

b) Establishing the source of wealth and funds; where the risk is particularly high and/or where the firm has doubts about the legitimate origin of the funds, verifying the source of wealth and funds may be the only adequate risk mitigation tool. The source of funds or wealth can be verified, by reference to, *inter alia*:

i. an original or certified copy of a recent pay slip;

ii. written confirmation of annual salary signed by an employer;

iii. an original or certified copy of contract of sale of, for example, investments or a company;

iv. written confirmation of sale signed by a lawyer or solicitor;

v. an original or certified copy of a will or grant of probate;

vi. written confirmation of inheritance signed by a lawyer, solicitor, trustee or executor;

vii. an internet search of a company registry to confirm the sale of a company;

viii. Performing greater levels of scrutiny and due diligence on business relationships than would be typical in mainstream financial service provision, such as in retail banking or investment management.

c) Establishing the destination of funds.

Guideline 13: Sectoral guideline for trade finance providers

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

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

a) 'Open account' transactions: these are transactions where the buyer makes a payment once they have received the goods. These are the most common means of financing trade, but the underlying trade-related nature of the transaction will often not be known to the banks executing the fund transfer. Banks should refer to the guidance in Title I to manage the risk associated with such transactions.

b) Documentary letters of credit (LCs) that have many variations and are suited to a different situation respectively: an LC is a financial instrument issued by a bank that guarantees payment to a named beneficiary (typically an exporter) upon presentation of certain 'complying' documents specified in the credit terms (e.g. evidence that goods have been dispatched).

c) Documentary bills for collection (BCs): a BC refers to a process by which payment, or an accepted draft, is collected by a 'collecting' bank from an importer of goods for onward payment to the exporter. The collecting bank gives the relevant trade documentation (which will have been received from the exporter, normally through their bank) to the importer in return.

13.3. Other trade finance products such as forfaiting or structured financing, or wider activity such as project finance, are outside the scope of these sectoral guidelines. Banks offering these products should refer to the general guidance in Title I.

13.4. Trade finance products can be abused for money laundering and terrorist financing purposes. For example, the buyer and seller may collude to misrepresent the price, type, quality or quantity of goods in order to transfer funds or value between countries.

13.5. Banks should take into account that the International Chamber of Commerce (ICC) has developed standards such as the Uniform Customs & Practice for Documentary Credits (600) that is a set of rules which apply to finance institutions which issue Letters of Credit that govern the use of LCs and BCs, but that these do not cover matters related to financial crime. Banks should note that these standards do not have legal force and their use does not mean that banks do not need to comply with their legal and regulatory AML/CFT obligations.

13.6. Firms in this sector should consider the following risk factors and measures alongside those set out in Title I of these guidelines. The sectoral guideline 8 in Title II may also be relevant in this context.

Risk factors

13.7. Banks that are party to trade finance transactions often have access only to partial information about the transaction and the parties to it. Trade documentation can be diverse, and banks may not have expert knowledge of the different types of trade documentation they receive. This can make the identification and assessment of ML/TF risk challenging.

13.8. Banks should, nevertheless, use common sense and professional judgement to assess the extent to which the information and documentation they have could give rise to concern or suspicion of ML/TF.

13.9. To the extent possible, banks should consider the following risk factors:

Transaction risk factors

13.10. The following factors may contribute to increasing risk:

a) The transaction is unusually large given what is known about a customer's previous line of business and trading activity.

b) The transaction is highly structured, fragmented or complex, involving multiple parties, without apparent legitimate justification

c) Copy documents are used in situations where original documentation would be expected, without reasonable explanation.

d) There are significant discrepancies in documentation, for example between the description of the type, quantity or quality of goods in key documents (i.e. invoices, insurance and transport documents) and actual goods shipped, to the extent that this is known.

e) The type, quantity and value of goods is inconsistent with the bank's knowledge of the buyer's business.

f) The goods transacted are higher risk for money-laundering purposes, for example certain commodities the prices of which can fluctuate significantly, which can make bogus prices difficult to detect.

g) The agreed value of goods or shipment is over- or under-insured or multiple insurances are used, to the extent this is known.

h) The goods transacted require export licenses, such as specific export authorizations for dual-use items that are goods, software and technology that can be used for both civilian and military applications.

i) The trade documentation does not comply with applicable laws or standards.

j) Unit pricing appears unusual, based on what the bank knows about the goods and trade.

k) The transaction is otherwise unusual, for example LCs are frequently amended without a clear rationale or goods are shipped through another jurisdiction for no apparent commercial reason.

l) The goods traded are destined to a party or country that is subject to a sanction, an embargo or a similar measure issued by, for example, the Union or the United Nations, or in support of such party or country.

13.11. The following factors may contribute to reducing risk:

a) Independent inspection agents have verified the quality and quantity of the goods and the presence of the necessary documents and authorisations.

b) Transactions involve established counterparties that have a proven track record of transacting with each other and due diligence has previously been carried out.

Customer risk factors

13.12. The following factors may contribute to increasing risk:

a) The transaction and/or the parties involved are out of line with what the bank knows about the customer's previous activity or line of business (e.g. the goods being shipped, or the shipping volumes, are inconsistent with what is known about the importer or exporter's business).

b) There are indications that the buyer and seller may be colluding, for example:

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

ii. transacting businesses have the same address, provide only a registered agent's address, or have other address inconsistencies;

iii. the buyer is willing or keen to accept or waive discrepancies in the documentation.

c) The customer is unable or reluctant to provide relevant documentation to support the transaction.

d) The customer faces difficulties explaining the rationale of the entire export process or is unable to explain the content and meaning of the underlying to the LC or BC documents.

e) The buyer´s legal structure does not allow the identification of its owners or it uses agents or third parties to represent the buyers rights and interests.

13.13. The following factors may contribute to reducing risk:

a) The customer is an existing customer whose business is well known to the bank and the transaction is in line with that business.

Country or geographical risk factors

13.14. The following factors may contribute to increasing risk:

a) A country associated with the transaction (including the country from which the goods originated, for which they are destined or transited through, or where either party to the transaction is based) has no currency exchange controls in place. This increases the risk that the transaction's true purpose is to export currency in contravention of local law.

b) A country associated with the transaction has higher levels of predicate offences (e.g. those related to the narcotics trade, smuggling or counterfeiting) or free trade zones.

c) Transaction is executed under auspices of governmental or international organizations or foundations to support the victims of natural disaster or persons affected from war conflict or civil unrest.

13.15. The following factors may contribute to reducing risk:

a) The trade is within the EU/EEA.

b) Countries associated with the transaction have an AML/CFT regime not less robust than that required under Directive (EU) 2015/849 and are associated with low levels of predicate offences.

Measures

13.16. Banks must carry out CDD on the instructing party. In practice, most banks will only accept instructions from existing customers and the wider business relationship that the bank has with the customer may assist its due diligence efforts.

13.17. Where a bank provides trade finance services to a customer, it should take steps, as part of its CDD process, to understand its customer's business . Examples of the type of information the bank could obtain include the countries with which the customer trades, the trading routes used, goods traded, who the customer does business with (buyers, suppliers, etc.), whether the customer uses agents or third parties, and, if so, where these are based. This should help banks understand who the customer is and aid the detection of unusual or suspicious transactions.

13.18. Where a bank is a correspondent, it must apply CDD measures to the respondent. Correspondent banks should follow the sectoral guideline 8 on correspondent banking.

Enhanced customer due diligence

13.19. To comply with Article 18a in respect of relationships or transactions involving high-risk third countries, firms should apply the EDD measures set out in this regard in Title I.

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

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

a) Taking steps to better understand the ownership or background of other parties to the transaction, in particular where they are based in a jurisdiction associated with higher ML/TF risk or where they handle high-risk goods. This may include checks of company registries and third party intelligence sources, and open source internet searches.

b) Obtaining more information on the financial situation of the parties involved.

13.22. Checks on transactions may include:

a) using third party or open source data sources, for example the International Maritime Bureau (for warning notices, bills of lading, shipping and pricing checks) or shipping lines' free container tracking service to verify the information provided and to check that the purpose of the transaction is legitimate;

b) using professional judgement to consider whether the pricing of goods makes commercial sense, in particular in relation to traded commodities for which reliable and up-to-date pricing information can be obtained;

c) checking that the weights and volumes of goods being shipped are consistent with the shipping method.

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

Simplified customer due diligence

13.24. The checks banks routinely carry out to detect fraud and ensure the transaction conforms to the standards set by the International Chamber of Commerce mean that, in practice, they will not apply SDD measures even in lower risk situations.

Guideline 14: Sectoral guideline for life insurance undertakings

14.1. Life insurance products are designed to financially protect the policy holder against the risk of an uncertain future event, such as death, illness or outliving savings in retirement (longevity risk). Protection is achieved by an insurer who pools the financial risks that many different policy holders are faced with. Life insurance products can also be bought as investment products or for pension purposes.

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

14.3. Most life insurance products are designed for the long term and some will only pay out on a verifiable event, such as death or retirement. This means that many life insurance products are not sufficiently flexible to be the first vehicle of choice for money launderers. However, as with other financial services products, there is a risk that the funds used to purchase life insurance may be the proceeds of crime.

14.4. Firms in this sector should consider the following risk factors and measures alongside those set out in Title I of these guidelines. The sectoral guidelines 12 and 16 in Title II may also be relevant in this context. Where intermediaries are used, the delivery channel risk factors set out in Title I will be relevant.

14.5. Intermediaries may also find these guidelines useful.

Risk factors

Product, service and transaction risk factors

14.6. The following factors may contribute to increasing risk:

a) Flexibility of payments, for example the product allows:

i. payments from unidentified third parties;

ii. high-value or unlimited-value premium payments, overpayments or large volumes of lower value premium payments;

iii. cash payments.

b) Ease of access to accumulated funds, for example the product allows partial withdrawals or early surrender at any time, with limited charges or fees.

c) Negotiability, for example the product can be:

i. traded on a secondary market;

ii. used as collateral for a loan.

d) Anonymity, for example the product facilitates or allows the anonymity of the customer.

14.7. Factors that may contribute to reducing risk include: The product:

a) only pays out against a pre-defined event, for example death, or on a specific date, such as in the case of credit life insurance policies covering consumer and mortgage loans, which only pay out on the death of the insured person;

b) has no surrender value;

c) has no investment element;

d) has no third party payment facility;

e) requires that total investment is curtailed at a low value;

f) is a life insurance policy where the premium is low;

g) only allows small-value regular premium payments, for example no overpayment;

h) is accessible only through employers, for example a pension, superannuation or similar scheme that provides retirement benefits to employees, where contributions are made by way of deduction from wages and the scheme rules do not permit the assignment of a member's interest under the scheme;

i) cannot be redeemed in the short or medium term, as in the case of pension schemes without an early surrender option;

j) cannot be used as collateral;

k) does not allow cash payments;

l) has conditions limiting the availability of funds that must be met to benefit from tax relief.

Customer and beneficiary risk factors

14.8. The following factors may contribute to increasing risk:

a) The nature of the customer, for example:

i. legal persons whose structure makes it difficult to identify the beneficial owner;

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

iii. the beneficiary of the policy or the beneficial owner of this beneficiary is a PEP;

iv. the customer's age is unusual for the type of product sought (e.g. the customer is very young or very old);

v. the contract does not match the customer's wealth situation;

vi. the customer's profession or activities are regarded as particularly likely to be related to money laundering, for example because they are known to be very cash intensive or exposed to a high risk of corruption;

vii. the contract is subscribed by a 'gatekeeper', such as a fiduciary company, acting on behalf of the customer;

viii. the policy holder and/or the beneficiary of the contract are companies with nominee shareholders and/or shares in bearer form.

b) The customer's behaviour:

i. In relation to the contract, for example:

a. the customer frequently transfers the contract to another insurer;

b. frequent and unexplained surrenders, especially when the refund is done to different bank accounts;

c. the customer makes frequent or unexpected use of 'free look' provisions/'cooling-off' periods in particular where the refund is made to an apparently unrelated third party;

d. the customer incurs a high cost by seeking early termination of a product;

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

f. the customer's request to change or increase the sum insured and/or the premium payment are unusual or excessive.

ii. In relation to the beneficiary, for example:

a. the insurer is made aware of a change in beneficiary only when the claim is made;

b. the customer changes the beneficiary clause and nominates an apparently unrelated third party;

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

iii. In relation to payments, for example:

a. the customer uses unusual payment methods, such as cash or structured monetary instruments or other forms of payment vehicles fostering anonymity;

b. payments from different bank accounts without explanation;

c. payments from banks that are not established in the customer's country of residence;

d. the customer makes frequent or high-value overpayments where this was not expected;

e. payments received from unrelated third parties;

f. catch-up contribution to a retirement plan close to retirement date.

14.9. The following factors may contribute to reducing risk. In the case of corporate-owned life insurance, the customer is:

a) a credit or financial institution that is subject to requirements to combat money laundering and the financing of terrorism and supervised for compliance with these requirements in a manner that is consistent with Directive (EU) 2015/849;

b) a public administration or a public enterprise from an EEA jurisdiction.

Distribution channel risk factors

14.10. The following factors may contribute to increasing risk:

a) non-face-to-face sales, such as online, postal or telephone sales, without adequate safeguards, such as electronic signatures or electronic identification means that comply with Regulation (EU) No 910/2014;

b) long chains of intermediaries;

c) an intermediary is used in unusual circumstances (e.g. unexplained geographical distance).

14.11. The following factors may contribute to reducing risk:

a) Intermediaries are well known to the insurer, who is satisfied that the intermediary applies CDD measures commensurate to the risk associated with the relationship and in line with those required under Directive (EU) 2015/849.

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

Country or geographical risk factors

14.12. The following factors may contribute to increasing risk:

a) The insurer, the customer, the beneficial owner, the beneficiary or the beneficial owner of the beneficiary are based in, or associated with, jurisdictions associated with higher ML/TF risk. Firms should pay particular attention to jurisdictions without effective AML/CFT supervision.

b) Premiums are paid through accounts held with financial institutions established in jurisdictions associated with higher ML/TF risk. Firms should pay particular attention to jurisdictions without effective AML/CFT supervision.

c) The intermediary is based in, or associated with, jurisdictions associated with higher ML/TF risk. Firms should pay particular attention to jurisdictions without effective AML/CFT supervision.

14.13. The following factors may contribute to reducing risk:

a) Countries are identified by credible sources, such as mutual evaluations or detailed assessment reports, as having effective AML/CFT systems.

b) Countries are identified by credible sources as having a low level of corruption and other criminal activity.

Measures

14.14. Article 13(5) of Directive (EU) 2015/849 provides that, for life insurance business, firms must apply CDD measures not only to the customer and beneficial owner but also to the beneficiaries as soon as they are identified or designated. This means that firms must:

a) obtain the name of the beneficiary where either a natural or legal person or an arrangement is identified as the beneficiary; or

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

14.15. Firms must verify the beneficiaries' identities at the latest at the time of payout.

14.16. Where the firm knows that the life insurance has been assigned to a third party, who will receive the value of the policy, they must identify the beneficial owner at the time of the assignment.

14.17. In order to comply with Article 13(6) of Directive (EU) 2015/849, when the beneficiaries of trusts or of similar legal arrangements are a class of persons or designated by certain characteristics, firms should obtain sufficient information to be satisfied that the identities of the beneficiaries can be established at the time of payout or at the time of the exercise by the beneficiaries of their vested rights.

Enhanced customer due diligence

14.18. To comply with Article 18a in respect of relationships or transactions involving high-risk third countries, firms should apply the EDD measures set out in this regard in Title I. The following EDD measures may be appropriate in all other high-risk situation:

a) Where the customer makes use of the 'free look'/'cooling-off' period, the premium should be refunded to the customer's bank account from which the funds were paid. Firms should ensure that they have verified the customer's identity in line with Article 13 of Directive (EU) 2015/849 before making a refund, in particular where the premium is large or the circumstances appear otherwise unusual. Firms should also consider whether the cancellation gives rise to suspicion about the transaction and whether submitting a suspicious activity report would be appropriate.

b) Additional steps may be taken to strengthen the firm's knowledge about the customer, the beneficial owner, the beneficiary or the beneficiary's beneficial owner, the third party payers and payees. Examples include:

i. not using the derogation in Article 14(2) of Directive (EU) 2015/849, which provides for an exemption from upfront CDD;

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

iii. obtaining additional information to establish the intended nature of the business relationship;

iv. obtaining additional information on the customer and updating more regularly the identification data of the customer and beneficial owner;

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

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

vii. establishing the customer's source of wealth and source of funds, for example employment and salary details, inheritance or divorce settlements;

viii. where possible, identifying the beneficiary and verifying their identity at the beginning of the business relationship, rather than waiting until they are identified or designated, bearing in mind that the beneficiary can change over the term of the policy;

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

x. in line with Articles 20 and 21 of Directive (EU) 2015/849, taking measures to determine whether the customer is a PEP and taking reasonable measures to determine whether the beneficiary or the beneficiary's beneficial owner is a PEP at the time of assignment, in whole or in part, of the policy or, at the latest, at the time of payout;

xi. requiring the first payment to be carried out through an account in the customer's name with a bank subject to CDD standards that are not less robust than those required under Directive (EU) 2015/849.

14.19. Article 20 of Directive (EU) 2015/849 requires that, where the risk associated with a PEP relationship is high, firms must not only apply CDD measures in line with Article 13 of the Directive but also inform senior management before the payout of the policy so that senior management can take an informed view of the ML/TF risk associated with the situation and

decide on the most appropriate measures to mitigate that risk; in addition, firms must conduct EDD on the entire business relationship.

14.20. Firms should:

a) obtain additional information on the business relationship so as to be able to understand the nature of the relationship between the customer/the insured and the beneficiary, and of the relationship between the payer and the beneficiary if the payer is different from the customer/the insured; and

b) enhance their scrutiny on the source of funds.

14.21. Where the beneficiary is a PEP and is expressly named, firms should not wait until the payout of the policy to conduct the enhanced scrutiny of the entire business relationship.

14.22. More frequent and more in-depth monitoring of transactions may be required (including where necessary, establishing the source of funds).

Simplified customer due diligence

14.23. The following measures may satisfy some of the CDD requirements in low-risk situations (to the extent permitted by national legislation):

a) Firms may be able to assume that the verification of the identity of the customer is fulfilled on the basis of a payment drawn on an account that the firm is satisfied is in the sole or joint name of the customer with an EEA-regulated credit institution.

b) Firms may be able to assume that the verification of the identity of the beneficiary of the contract is fulfilled on the basis of a payment made to an account in the beneficiary's name at a regulated EEA credit institution.

Guideline 15: Sectoral guideline for investment firms

15.1. Investment firms as defined in point (1) of Article 4(1) of Directive 2014/65/EUshould consider when providing or executing investment services or activities as defined in point (2) of Article 4(1) of Directive (EU) 2014/65 the following risk factors and measures alongside those set out in Title I of these guidelines. The sectoral guideline 12 may also be relevant in this context.

15.2. To comply with their obligations under Directive (EU) 2015/849, firms in this sector should consider that:

a) ML/TF risk in this sector is driven primarily by the risk associated with the clients whom investment firms serve; and

b) the nature of the activities which investment firms undertake means that they may be exposed to predicate offences such as market abuse, which may lead to ML/TF.

Risk factors

Product, service or transaction risk factors

15.3. The following factors may contribute to increasing risk:

a) transactions are unusually large, in the context of the customer's profile;

b) settlement arrangements that are non-standard or appear irregular;

c) mirror trades or transactions involving securities used for currency conversion that appear unusual or have no apparent business or economic purposes;

d) the product or service is structured in a way that may present difficulties in identifying the customers; third party payments are possible.

15.4. The following factors may contribute to reducing risk:

a) The product or service is subject to mandatory transparency and/or disclosure requirements.

Customer risk factors

15.5. The following factors may contribute to increasing risk:

a) The customer's behaviour, for example:

i. the rationale for the investment lacks an obvious economic purpose;

ii. the customer asks to repurchase or redeem a long-term investment within a short period after the initial investment or before the payout date without a clear rationale, in particular where this results in financial loss or payment of high transaction fees;

iii. the customer requests the repeated purchase and sale of shares within a short period of time without an obvious strategy or economic rationale

iv. unwillingness to provide CDD information on the customer and the beneficial owner;

v. frequent changes to CDD information or payment details;

vi. the customer transfers funds in excess of those required for the investment and asks for surplus amounts to be reimbursed;

vii. the circumstances in which the customer makes use of the 'cooling-off' period give rise to suspicion;

viii. using multiple accounts without previous notification, especially when these accounts are held in multiple or high-risk jurisdictions;

ix. the customer wishes to structure the relationship in such a way that multiple parties, for example nominee companies, are used in different jurisdictions, particularly where these jurisdictions are associated with higher ML/TF risk.

b) The customer's nature, for example:

i. the customer is a company, a trust or other legal arrangements having a structure or functions similar to trusts, established in a jurisdiction associated with higher ML/TF risk (firms should pay particular attention to those jurisdictions that do not comply effectively with international tax and information sharing transparency standards);

ii. the customer is an investment vehicle that carries out little or no due diligence on its own clients;

iii. the customer is an unregulated third party investment vehicle;

iv. the customer's ownership and control structure is opaque;

v. the customer or the beneficial owner is a PEP or holds another prominent position that might enable them to abuse their position for private gain;

vi. the customer is a non-regulated nominee company with unknown shareholders.

c) The customer's business, for example the customer's funds are derived from business in sectors that are associated with a higher risk of financial crime, such as construction, pharmaceuticals and healthcare, the arms trade and defence, the extractive industries or public procurement.

15.6. The following factors may contribute to reducing risk:

a) The customer is an institutional investor whose status has been verified by an EEA government agency, for example a government-approved pensions scheme.

b) The customer is a government body from an EEA jurisdiction.

c) The customer is a financial institution established in an EEA jurisdiction.

Distribution channel risk factors

15.7. The following factors may contribute to increasing the risk:

a) Complexity in the chain of reception and transmission of orders;

b) Complexity in the distribution chain of investment products;

c) The trading venue has members or participants located in high-risk jurisdictions

Country or geographical risk factors

15.8. The following factors may contribute to increasing risk:

a) The investor or their custodian is based in a jurisdiction associated with higher ML/TF risk.

b) The funds come from a jurisdiction associated with higher ML/TF risk.

Measures

15.9. When developing their AML/CFT policies and procedures to comply with their obligations under Directive (EU) 2015/849, firms in this sector should consider that depending on the type of activity they perform, they will be subject to rules under which they have to gather extensive information about their customers. Where this is the case, they should consider the extent to which information obtained for MiFID II and EMIR compliance purposes can be used also to meet their CDD obligations in standard situations.

15.10. In particular, investment managers typically need to develop a good understanding of their customers to help them identify suitable investment portfolios. The information gathered will be similar to that which firms obtain for AML/CFT purposes.

15.11. Firms should follow the EDD guidelines set out in Title I in higher risk situations. In addition, where the risk associated with a business relationship is high, firms should:

a) identify and, where necessary, verify the identity of the underlying investors of the firm's customer where the customer is an unregulated third party investment vehicle;

b) understand the reason for any payment or transfer to or from an unverified third party.

15.12. To the extent permitted by national legislation, investment managers may apply the SDD guidelines set out in Title I in low-risk situations.

Guideline 16: Sectoral guideline for providers of investment funds

16.1. The provision of investment funds can involve multiple parties, such as the fund manager, appointed advisers, the depositary and sub-custodians, registrars and, in some cases, prime brokers. Similarly, the distribution of these funds can involve parties such as tied agents, advisory and discretionary wealth managers, platform service providers and independent financial advisers.

16.2. The type and number of parties involved in the fund's distribution process depends on the nature of the fund and may affect how much the fund knows about its customer and investors. The fund or, where the fund is not itself an obliged entity, the fund manager will retain responsibility for compliance with AML/CFT obligations, although aspects of the fund's CDD obligations may be carried out by one or more of these other parties subject to certain conditions.

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

a) Retail funds are often distributed on a non-face-to-face basis; access to such funds is often easy and relatively quick to achieve, and holdings in such funds can be transferred between different parties.

b) Alterative investment funds, such as hedge funds, real estate and private equity funds, tend to have a smaller number of investors, which can be private individuals as well as institutional investors (pension funds, funds of funds). Such funds that are designed for a limited number of high-net-worth individuals, or for family offices, can have an inherently higher risk of abuse for ML/TF purposes than retail funds, since investors are more likely to be in a position to exercise control over the fund assets. If investors exercise control over the assets, such funds are personal asset-holding vehicles, which are mentioned as a factor indicating potentially higher risk in Annex III to Directive (EU) 2015/849.

c) Notwithstanding the often medium- to long-term nature of the investment, which can contribute to limiting the attractiveness of these products for money laundering purposes, they may still appeal to money launderers on the basis of their ability to generate growth and income.

16.4. This sectoral guideline is directed at:

a) investment funds marketing their own shares or units, under Article 3(2)(d) of Directive (EU) 2015/849; and

b) funds managers, where an investment fund is not incorporated.

Other parties involved in the provision or distribution of the fund, for example intermediaries, may have to comply with their own CDD obligations and should refer to relevant chapters in these guidelines as appropriate.

For funds and fund managers, the sectoral guidelines 8, 14 and 15 may also be relevant.

Risk factors

Product, service or transaction risk factors

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

a) The fund is designed for a limited number of individuals or family offices, for example a private fund or single investor fund.

b) It is possible to subscribe to the fund and then quickly redeem the investment without the investor incurring significant administrative costs;

c) Units of or shares in the fund can be treated without the fund or fund manager being notified at the time of the trade;

d) Information about the investor is divided among several subjects.

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

a) The subscription involves accounts or third parties in multiple jurisdictions, in particular where these jurisdictions are associated with a high ML/TF risk as defined in guideline 2.9 to 2.15 of Title I.

b) The subscription involves third party subscribers or payees, in particular where this is unexpected.

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

a) Payments to and from third parties are not allowed.

b) The fund is open to small-scale investors only, with investments capped.

Customer risk factors

16.8. The following factors may contribute to increasing risk. The customer's behaviour is unusual, for example:

a) The rationale for the investment lacks an obvious strategy or economic purpose or the customer makes investments that are inconsistent with the customer's overall financial situation, where this is known to the fund or fund manager.

b) The customer requests the repeated purchase and/or sale of units or shares within a short period of time after the initial investment or before the payout date without a clear strategy or rationale, in particular where this results in financial loss or payment of high transaction fees.

c) The customer transfers funds in excess of those required for the investment and asks for surplus amounts to be reimbursed.

d) The customer uses multiple accounts without previous notification, especially when these accounts are held in multiple jurisdictions or jurisdictions associated with higher ML/TF risk.

e) The customer wishes to structure the relationship in such a way that multiple parties, for example non-regulated nominee companies, are used in different jurisdictions, particularly where these jurisdictions are associated with higher ML/TF risk.

f) The customer suddenly changes the settlement location without rationale, for example by changing the customer's country of residence.

16.9. The following factors may contribute to reducing risk:

a) the customer is an institutional investor whose status has been verified by an EEA government agency, for example a government-approved pensions scheme;

b) the customer is a firm subject to AML/CFT requirements that are not less robust than those required by Directive (EU) 2015/849.

Distribution channel risk factors

16.10. The following factors may contribute to increasing risk:

a) Complex distribution channels that limit the fund's oversight of its business relationships and restrict its ability to monitor transactions, for example the fund uses a large number of sub-distributors for distribution in third countries;

b) the distributor is located in a jurisdiction associated with higher ML/TF risk as defined in the general part of these guidelines.

16.11. The following factors may indicate lower risk:

a) The fund admits only a designated type of low-risk investor, such as regulated firms investing as a principal (e.g. life companies) or corporate pension schemes.

b) The fund can be purchased and redeemed only through a firm subject to AML/CFT requirements that are not less robust than those required by Directive (EU) 2015/849.

Country or geographical risk factors

16.12. The following factors may contribute to increasing risk:

a) The customers' or beneficial owners' funds have been generated in jurisdictions associated with higher ML/TF risk, in particular those associated with higher levels of predicate offences to money laundering.

b) The customer requests their investment to be redeemed to an account in a credit institution located in a jurisdiction associated with higher ML/TF risk.

Measures

16.13. The measures funds or fund managers should take to comply with their CDD obligations will depend on how the customer or the investor (where the investor is not the customer) comes to the fund. The fund or fund manager should also take risk-sensitive measures to identify and verify the identity of the natural persons, if any, who ultimately own or control the customer (or on whose behalf the transaction is being conducted), for example by asking the prospective customer to declare, when they first apply to join the fund, whether they are investing on their own behalf or whether they are an intermediary investing on someone else's behalf.

16.14. The customer is:

a) a natural or legal person who directly purchases units of or shares in a fund on their own account, and not on behalf of other, underlying investors; or

b) a firm that, as part of its economic activity, directly purchases units of or shares in its own name and exercises control over the investment for the ultimate benefit of one or more third parties who do not control the investment or investment decisions; or

c) a firm, for example a financial intermediary, that acts in its own name and is registered in the fund's share/units register but acts on the account of, and pursuant to specific instructions from, one or more third parties (e.g. because the financial intermediary is a nominee, broker, multi-client pooled account/omnibus type account operator or operator of a similar passive-type arrangement); or

d) a firm's customer, for example a financial intermediary's customer, where the firm is not registered in the fund's share/units register (e.g. because the

investment fund uses a financial intermediary to distribute fund shares or units, and the investor purchases units or shares through the firm and is registered in the fund's share/units register).

Enhanced Customer Due Diligence

16.15. In the situations described in guidelines 16.14 (a) and (b), examples of EDD measures a fund or fund manager should apply in high-risk situations include:

a) obtaining additional customer information, such as the customer's reputation and background, before the establishment of the business relationship;

b) taking additional steps to further verify the documents, data or information obtained;

c) obtaining information on the source of funds and/or the source wealth of the customer and of the customer's beneficial owner;

d) requiring that the redemption payment is made through the initial account used for investment or an account in the sole or joint name of the customer;

e) increasing the frequency and intensity of transaction monitoring;

f) requireng that the first payment is made through a payment account held in the sole or joint name of the customer with an EEA-regulated credit or financial institution or a regulated credit or financial institution in a third country that has AML/CFT requirements that are not less robust than those required by Directive (EU) 2015/849;

g) obtaining approval from senior management at the time the first transaction;

h) enhanced monitoring of the customer relationship and individual transactions.

16.16. In the situations described in guideline 16.14 (c), where the risk is increased, in particular where the fund is designated for a limited number of investors, EDD measures must apply and may include those set out in guideline 16.15 above.

16.17. Where a financial intermediary is based in a third country and has established a relationship similar to correspondent banking with the fund or the fund's manager, the measures described in guidelines 16.20 and 16.21 are not applicable. In such cases, to discharge their obligations under Article 19 of the Directive (EU) 2015/849, firms should apply toward the intermediary the enhanced due diligence measures listed in Sectoral Guideline 8. 14 to 8.17.

16.18. In the situations described in guideline 16.14(d) where the risk is increased, in particular where the fund is designated for a limited number of investors, EDD measures must apply and may include those set out in guideline 16.15 above.

Simplified Customer Due Diligence

16.19. In the situations described in guidelines 16.14 (a) and 16.14 (b), in lower risk situations, to the extent permitted by national legislation, and provided that the funds are verifiably being transferred to or from a payment account held in the customer's sole or joint name with an EEA-regulated credit or financial institution, an example of the SDD measures the fund or fund manager may apply is using the source of funds to meet some of the CDD requirements.

16.20. In the situations described in guideline 16.14(c) , where the financial intermediary is the fund or fund manager's customer, the fund or fund manager should apply risk-sensitive CDD measures to the financial intermediary. The fund or fund manager should also take risk-sensitive measures to identify, and verify the identity of, the investors underlying the financial intermediary, as these investors could be beneficial owners of the funds invested through the intermediary. To the extent permitted by national law, in low-risk situations, funds or fund managers may apply SDD measures similar to those described in Title I of these guidelines, subject to the following conditions:

a) The financial intermediary is subject to AML/CFT obligations in an EEA jurisdiction or in a third country that has AML/CFT requirements that are not less robust than those required by Directive (EU) 2015/849.

b) The financial intermediary is effectively supervised for compliance with these requirements.

c) The fund or fund manager has taken risk-sensitive steps to be satisfied that the ML/TF risk associated with the business relationship is low, based on, *inter alia*, the fund or fund manager's assessment of the financial intermediary's business, the types of clients the intermediary's business serves and the jurisdictions the intermediary's business is exposed to.

d) The fund or fund manager has taken risk-sensitive steps to be satisfied that the intermediary applies robust and risk-sensitive CDD measures to its own customers and its customers' beneficial owners. As part of this, the fund or fund manager should take risk-sensitive measures to assess the adequacy of the intermediary's CDD policies and procedures, for example by referring to publicly available information about the intermediary's compliance record or liaising directly with the intermediary.

e) The fund or fund manager has taken risk-sensitive steps to be satisfied that the intermediary will provide CDD information and documents on the underlying investors immediately upon request, for example by including relevant provisions in a contract with the intermediary or by sample-testing the intermediary's ability to provide CDD information upon request.

16.21. In the situations described in guideline 16.14 (d), the fund or fund manager should apply risk-sensitive CDD measures to the ultimate investor as the fund or fund manager's customer. To meet its CDD obligations, the fund or fund manager may rely upon the intermediary in line with, and subject to, the conditions set out in Chapter II, Section 4, of Directive (EU) 2015/849.

16.22. To the extent permitted by national law, in low-risk situations, funds or fund managers may apply SDD measures. Provided that the conditions listed in guideline 16.20 are met, SDD measures may consist of the fund or fund manager obtaining identification data from the fund's share register, together with the information specified in Article 27(1) of Directive (EU) 2015/849, which the fund or fund manager must obtain from the intermediary within a reasonable timeframe. The fund or fund manager should set that timeframe in line with the risk-based approach.

Guideline 17 Sectoral guideline for regulated crowdfunding platforms

17.1. For the purposes of this sectoral Guideline, the following definitions set out in Article 2(1) of Regulation (EU) 2020/1503 are used and should apply: 'crowdfunding service', 'crowdfunding platform', 'crowdfunding service provider' (CSP), 'project owner' and 'investor'. This sectoral Guideline refers to 'customers' in the meaning of 'clients', as defined in Article 2(1) (g) of that same regulation.

17.2. CSPs should recognise the risks arising from the borderless nature of crowdfunding platforms where the CSP's customers can be located anywhere in the world, including high-risk jurisdictions. CSPs should know their customers to prevent their crowdfunding platforms from being used to fund fictitious investment projects with illicit funds or being misused for TF purposes where a fictitious reason is given for a crowdfunding project, which never materialises and the funds obtained from crowdfunding are then used to finance a terror attack.

17.3. CSPs should consider the risk factors and measures set out in this sectoral guideline in addition to those set out in Title I. CSPs that provide investment services should also refer to the sectoral guidance 16.

Risk factors

Product, service and transaction risk factors

17.4. CSP should take into account the following risk factors as potentially contributing to increased risk:

a) The CSP collects funds through the crowdfunding platform but allows for later onward transmission, including business models where:

i. money is collected for an undetermined project and consequently held in the investor's account until the project is determined; or

ii. money is collected but may be returned to the investors where the fundraising target is not met, or where the project owner has not received the money.

b) The CSP permits early redemption of investments, early repayment of loans, or resale of the investments or loans through secondary markets.

c) The CSP places no restriction on the size, volume or value of the transactions, loading or redemption processed through the crowdfunding platform, or the amount of funds to be stored in individual investor accounts.

d) The CSP allows investors to make a payment to the project owner through the crowdfunding platform with instruments, which are either outside the scope of any regulatory regime, or are subject to less robust AML/CFT requirements than those required by Directive (EU) 2015/849.

e) The CSP accepts cash investments from or permits cash withdrawals by investors that are individuals or unregulated legal entities through the crowdfunding platform.

f) The CSP provides for investors or lenders financial leverage or privileged redemption or guaranteed return.

g) The CSP does not confirm its commitment to buy back securities and there is no time for such buy-back.

h) For non-equity instruments, the nominal interest rate, the date from which interest becomes payable, the due dates for interest payments, the maturity date and the applicable yield are not understandably provided.

i) The CSP allows payments through the crowdfunding platform in virtual currencies.

j) The CSP allows investors and project owners to maintain multiple accounts on the crowdfunding platform where they are not linked to specific crowdfunding projects.

k) The CSP allows transfers between investors or project owners on the crowdfunding platform.

17.5. The CSP should take into account the following risk factors as potentially contributing to reduced risk:

a) The CSP requires that funds for investment, redemption, lending, or repayment are verifiably drawn from, or sent to, an account held in the customer's sole or joint name at a credit institution or financial institution, or a payment institution authorised under Directive (EU) 2015/2366, subject to AML/CFT requirements not less robust than those required by Directive (EU) 2015/849.

b) The CSP sets low-value limits on investment, lending, redemption, and repayment processed through the crowdfunding platform, in terms of monetary size and number of payments.

c) The CSP requires a fixed or longer holding period for investments, or repayment period for loans acquired through the crowdfunding platform.

d) The CSP limits the amount of funds that can be stored in any account at any one time on the crowdfunding platform.

e) The CSP utilises technology to spot whether the investors or project owners use VPN or other technologies that hide the real location and device when using the crowdfunding platform.

f) The CSP does not allow the creation of multiple accounts on the crowdfunding platform.

Customer risk factors

17.6. The CPS should take into account the following risk factors as potentially contributing to increased risk:

a) The customer's nature or behaviour is unusual, for example:

i. The rationale for the investment or loan lacks an obvious strategy or economic purpose.

ii. The investor asks to redeem an investment within a short period after the initial investment.

iii. The investor asks for privileged conditions or for fixed return on investment.

iv. The investor or the project owner transfers funds to the platform in excess of those required for the project/loan, and then asks for surplus amounts to be reimbursed;

v. The investor or the project owner is an individual or a legal person associated with higher levels of ML risks;

vi. The project owner accelerates, unexpectedly or without reasonable explanation, an agreed redemption/repayment schedule, by means either or lump sum payments or early termination; or

vii. The project owner appears to be reluctant in providing information about the project or initiative seeking crowdfunding.

viii. The source of the funds for the investment is unclear and the investor is reluctant to provide this information when requested by the CSP. The degree of invested assets exceeds the volume of the investor's estimated liquid assets. The funds invested are borrowed.

ix. Investor is not residing at or does not have any other connections with the country of the crowdfunding platform or the object of the investment.

x. Investor or project owner is a PEP.

xi. Investor is refusing to provide the required CDD.

b) The investor or the project owner transfer virtual currency.

c) The investor or the project owner were involved in negative news.

d) The investor or the project owner are under sanctions.

Distribution channel risk factors

17.7. The CSP should take into account the following risk factors as potentially contributing to increased risk

a) The CSP operates the crowdfunding platform entirely online without adequate safeguards, such as electronic identification of a person using electronic signatures or electronic identification means that comply with Regulation (EU) No 910/2014.

b) Customers are on-boarded non-face-to-face through the crowdfunding platform without any safeguards in place.

c) The CSP is operating outside any regulatory regime, and therefore the measures which would otherwise be in place to detect and mitigate potential use of the crowdfunding platform for ML/TF purposes may not be in place. This is without prejudice to the application of Guideline 11.

17.8. The CSP should take into account the following risk factors as potentially contributing to decreased risk:

a) The CSP uses a credit institution or financial institution to perform money handling or remittance services. Alternatively, the CSP opens an account in its own name in a regulated credit institution or financial institution, through which money transactions flow between project owners and investors.

b) The CSP operating the crowdfunding platform is authorised as a payment institution under Directive (EU) 2015/2366 or acts as an agent of a payment institution authorised under Directive (EU) 2015/2366 and directly processes money transactions among investors and project owners. This is without prejudice to the application of Guideline 11.

c) Investors and project owners have been met face-to-face or have been introduced by a regulated financial intermediary (credit institution or investment firm) who has carried out a full CDD on all the customers (project owners and investors)

Country or geographical risk factors

17.9. The CSP should take into account the following risk factors as potentially contributing to increased risk:

a) The CSP has a global reach, matching investors, project owners and projects from different jurisdictions.

b) The funds are derived from personal or business links to a jurisdiction identified by credible sources as having significant levels of corruption or other criminal activities, such as terrorism, money laundering, production and supply of illicit drugs, or other predicate offences.

c) The project owner or the investor, or their respective beneficial owners, where relevant, are located in a jurisdiction associated with higher ML/TF risks, or one without effective AML/CFT supervision. CSPs should pay particular attention to jurisdictions known to provide funding or support for terrorist activities or where groups committing terrorist offences are known to be operating, and jurisdictions subject to financial sanctions, embargoes or measures (issued, for example, by the EU or the United Nations) related to terrorism, financing of terrorism, or proliferation.

Measures

17.10. CSPs that are obliged entities as payment institutions authorised under Directive (EU) 2015/2366 or act as an agent of a payment institution authorised under Directive (EU) 2015/2366 should apply relevant measures in sectoral guideline 11 also to their crowdfunding services.

17.11. CSPs that are obliged entities as investment firms authorised under Directive (EU) 2014/65 should apply relevant measures in sectoral guideline 15 also to their crowdfunding services.

17.12. CSPs that are obliged entities as credit institutions authorized under Directive (EU) 2013/36 should apply relevant measures in sectoral guideline 9 also to their crowdfunding services.

17.13. An undertaking authorised as a CSP under national law and that is subject to national AML/CFT law should apply this sectoral guideline and other relevant sectoral guidelines *mutatis mutandis* in order to ensure harmonised and effective AML/CFT supervision of CSPs established in the Union.

Customer due diligence

17.14. CSPs should apply CDD measures in line with Title I to all their customers, be them investors or project owners.

17.15. CSPs that rely on credit institutions or financial institutions to collect funds from or transfer funds to customer, should refer to the distribution channel risk factors in Title I and in particular, satisfy themselves that these credit institutions or financial institutions have put in place appropriate customer due diligence measures.

Enhanced customer due diligence

17.16. Where the risk associated with an occasional transaction or a business relationship is increased CSPs platform should apply the following EDD measures:

a) obtaining additional information from the customers transacting on the platform, such as their investment intention and experience, background and reputation, before the establishment of the business relationship (for example, by carrying out open source or adverse media searches or commissioning a third party intelligence report to build a more complete customer profile);

b) taking additional steps to further verify the documents, data, or information obtained;

c) obtaining information on the source of funds of the customers and their beneficial owners;

d) requiring that the redemption payment or loan repayment is made through the initial account used for investment or an account in the sole or joint name of the customers concerned;

e) increasing the frequency and intensity of transaction monitoring;

f) requiring that the first payment of the investment or loan to be made through a payment account held in the sole or joint name of the party concerned with an EEA-regulated credit or financial institution or a regulated credit or financial

institution in a third country that has AML/CFT requirements not less robust than those required by Directive (EU) 2015/849;

g) obtaining approval from senior management at the time of the transaction when a customers uses the platform for the first time;

h) enhanced monitoring of the customer relationship and individual transactions.

Simplified customer due diligence

17.17. In low-risk situations, and to the extent permitted by national legislation, crowdfunding platforms may apply SDD measures, which may include:

a) verifying the customer's and, where applicable, the beneficial owner's identities during the establishment of the business relationship, in accordance with Article 14(2) of Directive (EU) 2015/849; or

b) assuming that a payment drawn on an account in the sole or joint name of the customer at a regulated credit or financial institution in an EEA country satisfies the requirements stipulated by Article 13(1)(a) and (b) of Directive (EU) 2015/849.

Guideline 18: Sectoral guideline for payment initiation service providers (PISPs) and account information service providers (AISPs)

18.1. When applying this Guideline, firms should have regard to the definitions in point 18 and 19 of Article 4 of Directive (EU) 2015/2366 in accordance with which:

a) a payment initiation service provider (PISP) is a payment service provider pursuing payment initiation services which in accordance with the definition in point 15 of Article 4 of Directive (EU) 2015/2366 means services to initiate a payment order at the request of the payment service user with respect to a payment account held at another payment service provider);

b) an account information service provider (AISP) is a payment service provider offering account information services which in accordance with the definition in point 16 of Article 4 of Directive (EU) 2015/2366 means online services to provide consolidated information on one or more payment accounts held by the payment service user with either another payment service provider or with more than one payment service provider).

18.2. Firms should take into account that despite PISPs and AISPs being obliged entities under Directive (EU) 2015/849, the inherent ML/TF risk associated with them is limited due to the fact that :

a) PISPs, although being involved in the payment chain, do not execute themselves the payment transactions and do not hold payment service users' (PSUs') funds;

b) AISPs are not involved in the payment chain and do not hold payment service user's funds.

18.3. When offering payment initiation services or account information services, PISPs and AISPs should take into account, together with Title I, the provision set out in this sectoral guideline.

Risk factors

Customer risk factors

18.4. When assessing ML/TF risks, PISPs and AISPs should take into account at least the following factors as potentially contributing to increased risk:

a) For PISPs: The customer transfers funds from different payment accounts to the same payee that, together, amount to a large sum without a clear economic or legitimate rationale, or that give the PISP reasonable grounds to suspect that the customer is trying to evade specific monitoring thresholds;

b) For AISPs: the customer transfers funds from different payment accounts to the same

payee, or receives funds on different payments accounts from the same payer, that, together, amount to a large sum without a clear economic or legitimate rationale, or that gives the AISP reasonable grounds to suspect that the customer is trying to evade specific monitoring thresholds.

Distribution channel risk factors

18.5. When assessing ML/TF risks, PISPs and AISPs may wish to refer to the ESAs' Opinion on the use of innovative solution in the customer due diligence process (JC 2017 81).

Country or geographical risk factor

18.6. When assessing ML/TF risks, PISPs and AISPs should at least take into account the following factors as potentially contributing to increased risk in particular if the customer uses multiple accounts held with different ASPSPs to make payments:

a) For PISPs: the customer initiates a payment to a jurisdiction associated with higher ML/TF risk or a high-risk third country or someone with known links to those jurisdictions.

b) For AISPs: The customer receives funds from, or sends funds to, jurisdictions associated with higher ML/TF risk or a high-risk third country or from/to someone with known links to those jurisdictions, or the customer connects payment accounts held in the name of multiple persons in more than one jurisdiction..

18.7. When assessing ML/TF risks, AISPs and PISPs should take into account the following factors as potentially contributing to decreased risk:

a) For PISPs: the customer initiates a payment transaction to an EEA member country or to third country that has AML/CFT requirements that are not less robust than those required by Directive (EU) 2015/849.

b) For AISPs: the customer's payment accounts are held in an EEA member country.

Measures

18.8. The customer is:

a) For PISPs: the customer is the natural or legal person who holds the payment account and requests the initiation of a payment order from that account. In the specific case where the PISP has a business relationship in the meaning of Article 3(13) of Directive (EU) 2015/849 with the payee for offering payment initiation services, and not with the payer, and the payer uses the respective PISP to initiate a single or one-off transaction to the respective payee, the PISPs' customer for the purpose of these Guidelines is the payee, and not the payer. This is without prejudice to Article 11 of Directive (EU) 2015/849 and Title I of these guidelines especially with regards to occasional transactions, and the PISPs' obligations under Directive (EU) 2015/2366 and other applicable EU legislation.

b) For AISPs: the customer is the natural or legal person who has the contract with the AISP. This can be the natural or legal person who holds the payment account(s).

18.9. PISPs and AISPs should take adequate measures to identify and assess the ML/TF risk associated with their business. To this end, PISPs and AISPs should take into account all data available to them. The type of data available to them will depend, *inter alia*, on the specific service offered to the customer, with the explicit consent of the payment service user and which is necessary for the provision of their services, in accordance with Article 66(3), letter (f) and Article 67(2), letter (f) of Directive (EU) 2015/2366.

18.10. Considering Article 11 of Directive (EU) 2015/849, PISPs and AISPs should determine the extent of CDD measures on a risk-sensitive basis, taking into account all data available to them with the explicit consent of the payment service user and which is necessary for the provision of their services, in accordance with Article 66(3), letter (f) and Article 67(2), letter (f) of Directive (EU) 2015/2366. In most cases, the low level of inherent risk associated with these business models means that SDD will be the norm. With regards to those cases of low risk and to the extent the application of SDD measures is prohibited or restricted under national law, AISPs and PISPs may adjust their CDD measures and apply guideline 18.15 accordingly.

18.11. Monitoring: As part of their CDD processes, PISPs and AISPs should ensure that their AML/CFT systems are set up in a way that alerts them to unusual or suspicious transactional activity, taking into account all data available to them with the explicit consent of the payment service user and which is necessary for the provision of their services, in accordance with Article 66(3), letter (f) and Article 67(2), letter (f) of Directive (EU) 2015/2366. PISPs and AISPs should use their own, or third party typologies, to detect unusual transactional activity.

Customer due diligence

18.12. PISPs and AISPs should apply the CDD measures to their customers in line with Title I.

18.13. Pursuant to Article 13 of Directive (EU) 2015/849 each time an account is added, the AISP should ask the customer, or verify through other means, whether the account is his own account, a shared account, or a legal entity's account for which the customer has a mandate to access (e.g.: an association, a corporate account).

Enhanced customer due diligence

18.14. In higher risk situations, firms should apply the EDD measures set out in Title I.

Simplified customer due diligence

18.15. Firms should always know the name of their customer. PISPs and AISPs and may consider applying SDD such as:

a) Relying on the source of funds as evidence of the customer's identity where the payment account details of the customer are known, and the payment account is held at an EEA-regulated payment service provider;

b) Postponing the verification of the customer's identity to a certain later date after the establishment of the relationship. In that case, firms should ensure that their policies and procedures set out at what point CDD should be applied;

c) Assuming the nature and purpose of the business relationship;

Guideline 19: Sectoral guideline for firms providing activities of currency exchange offices

19.1. Firms providing currency exchange services should take into account, together with Title I, the provisions referred to in this Guideline.

19.2. Firms should have regard to the inherent risks of the currency exchange services which may expose them to significant ML/TF risks. Firms should be aware that these risks stem from the simplicity of transactions, their speed and their often cash-based character. Firms should also have regard to the fact that their understanding of the ML/TF risk associated with the customer may be limited due to the fact that they usually carry out occasional transactions rather than establish a business relationship.

Risk factors

Product, service and transaction risk factors

19.3. Firms should take into account the following factors as potentially contributing to increased risk:

a) The transaction is unusually large in absolute terms or compared with the economic profile of the customer;

b) The transaction has no apparent economic or financial purpose;

19.4. Firms should take into account the following factors as potentially contributing to reduced risk:

a) The amount changed is low; firms should note that low amounts alone will not be enough to discount TF risk;

Customer risk factors

19.5. Firms should take into account the following factors as potentially contributing to increased risk:

a) The customer behaviour :

i. the customer's transactions are just below the applicable threshold for CDD, in particular where these are frequent or within a short period of time;

ii. the customer cannot or will not provide information about the origin of the funds;

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

iv. the customer exchanges large quantities of low denomination notes in one currency for higher denominations notes in another currency; or vice versa.

v. The customer's behaviour makes no apparent economic sense;

vi. The customer visits many premises of the same firm in the same day (To the extent that it is known by the firm);

vii. The customer enquiries about identification threshold and/or refuses to answer casual or routine questions;

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

ix. Exchange of large amounts or frequent exchanges that are not related to the customer's business;

x. The currency sold by the customer is inconsistent with his or her country of citizenship or residence;

xi. The customer buys currency from an unusual location in comparison to his/her own location without any logical explanation;

xii. The customer buys currency that does not fit with what is known about the customer's country of destination;

xiii. The customer buys or sells a large amount of a currency from a jurisdiction associated with significant levels of predicate offences to ML or terrorist activity;

b) The customer's business activity:

i. The customer business is associated with a higher ML/TF risk for example casinos, purchase/sale of precious metal and precious stones, scrap dealer;

Distribution channel risk factors

19.6. Firms should take into account the following factors as potentially contributing to increased risk:

a) The service is provided entirely online without adequate safeguards;

b) The provision of services is conducted through an agent network

Country or geographical risk factors

19.7. Firms should take into account the following factors as potentially contributing to increased risk:

a) The bureau de change business is located in a jurisdiction associated with higher ML/TF risk;

Measures

19.8. Since this business is primarily transaction-based, firms should consider which monitoring systems and controls they put in place to ensure that they are able to detect money-laundering and terrorist financing attempts, even where the CDD information they hold on the customer is basic or missing. This monitoring system should be adapted to the business volume and the risk exposure.

Customers due diligence

19.9. Firms should clearly define in their internal policies and procedures at what point they should carry out CDD to their occasional customers. This should encompass:

a) The situation where a transaction or identified linked transactions amount to EUR 15 000, or to the national threshold(s) if lower, or more. The policies and procedures should clearly define at what point a series of one-off transactions amounts to a business relationship taking into account the context of the firms'activities (i.e. the average normal size of a one-off transaction by their normal clientele).

b) The situation where there is a suspicion of money laundering or terrorist financing.

19.10. Firms should in any case put in place systems and controls in accordance with guideline 4.7 (b) to:

a) identify linked transactions (for example, to detect whether the same customer approaches multiple offices in a short space of time);

b) monitor transactions in a way that is adequate and effective in light to the size of the firm, the number of its offices, the size and volume of transactions; the type of activities performed, its delivery channels and the risks identified in its business-wide risk assessment.

Enhanced customer due diligence

19.11. Where the risk associated with an occasional transaction or business relationship is increased, firms should apply EDD in line with Title I, including, where appropriate, increased

transaction monitoring (e.g. increased frequency or lower thresholds), obtaining more information about the nature and purpose of the business, or the source of the customer's funds.

Simplified customer due diligence

19.12. To the extent permitted by national legislation, firms may consider applying SDD in low- risk situations such as:

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

b) verifying the customer's identity on the basis of a payment drawn on an account in the sole or joint name of the customer with an EEA-regulated credit or financial institution.

Guideline 20: Sectoral guideline for corporate finance

20.1. Firms providing corporate finance services should take into account the inherent ML/TF risks linked with these activities and be mindful that such activity is based on close advisory relationships in particular with corporate clients and other parties such as potential strategic investors.

20.2. When offering corporate finance services, firms should apply Title I and additionally the provisions set out in this Guideline. The sectoral guidelines 12, 15 and 16 may also be relevant in this context.

Risk factors

Customer and beneficiary risk factors

20.3. Where offering corporate finance services, firms should take into account the following risk factors as potentially contributing to increased risk:

a) the ownership of the customer is opaque without any obvious commercial or lawful rationale. For example, where ownership or control is vested in other entities such as trusts or Securitisation special purpose entities as defined in Article 2(2) of Regulation (EU) 2017/2402 (SSPE);

b) corporate structures or transactions are complex such as a long holding chain with use of front companies, or a lack transparency, and this appears to be for no reasonable business purpose;

c) where there is no evidence the customer has received a mandate or a sufficiently senior management approval to conclude the contract;

d) there are few independent means of verification of the customer's identity;

e) misconduct such as securities fraud or insider trading is suspected.

20.4. Where offering corporate finance services, firms should take into account the following risk factors as potentially contributing to reduced risk. The customer is:

a. a public administration or enterprise from a jurisdiction with low levels of corruption; or

b. a credit or financial institution from a jurisdiction with an effective AML/CFT regime, and is supervised for compliance with their AML/CFT obligations.

Country or geographical risk factors

20.5. Where offering corporate finance services, firms should take into account the following risk factors as potentially contributing to increased risk:

a. the customer or their beneficial owner is based in, or associated with, jurisdictions associated with higher ML/TF risk. Firms should pay particular attention to jurisdictions with high levels of corruption.

Measures

20.6. Providers of corporate finance will, by the nature of the business, be gathering substantial due diligence information as a matter of course; firms should draw upon this information for AML/CFT purposes.

Enhanced customer due diligence

20.7. Where the risk associated with a business relationship or an occasional transaction is increased, firms should apply EDD measures such as:

a) Additional checks on customers' ownership and control structure, beneficial ownership, and in particular any links the customer might have with politically exposed persons, and the extent to which these links affect the ML/TF risk associated with the business relationship;

b) Assessments of the integrity of directors, shareholders, and other parties with significant involvement in the customer's business and the corporate finance transaction;

c) Verification of the identity of other owners or controllers of a corporate entity;

d) Establishing the source and nature of the funds or assets involved by all the parties to the transaction, where appropriate through evidence or assurances from appropriate third parties.

e) Additional checks in order to establish the financial situation of the corporate client;

f) Use of non-documentary forms of evidence, such as meetings with credible persons who know the individuals in question; such as bankers, auditors or legal advisors. Firms should consider if this evidence is sufficient to demonstrate that the customer has correctly represented their personal and financial circumstances. Where non-documentary evidence of this sort is used, a record setting out the basis on which decisions were reached should be kept;

g) Risk-sensitive customer due diligence checks on other parties to a financial arrangement to gain sufficient background knowledge to understand the nature of the transaction. This is because money laundering risks may be posed to the firm not only by its customers, but also by parties to transactions with whom the firm does not have a direct business relationship. Firms should have regard to the fact that those parties may include:

i. the take-over or merger target of a client firm;

ii. potential or actual investors in a corporate client;

iii. corporate entities in which the firm takes a substantial ownership stake (but with which it does not have a wider business relationship);

iv. potential future customers;

v. in securitization transactions as defined in Article 2(1) of Regulation (EU) 2017/2402: agents acting on behalf of the SSPE (who may or may not be a regulated entity);

h) Firms offering corporate finance services should apply enhanced ongoing monitoring. In that regard, firms that use automated transaction monitoring should combined it with the knowledge and expertise of staff engaged in the activity. This enhanced monitoring should result in a clear understanding of why a customer undertakes a particular transaction or activity; for this purpose, firms should ensure that their staff use their knowledge of the customer, and what would be normal in the given set of circumstances, to be able to spot the unusual or potentially suspicious.

i) When taking part in securities' issuance, the firm should confirm that third-parties participating in selling securitisation instruments or transactions to investors have sufficient customer due diligence arrangements of their own in place.

j) In considering the ML/TF risks associated with a securitisation instruments or transaction, a firm should understand the underlying economic purpose of the arrangement, including the level of due diligence appropriate for different parties to the arrangement, which may include parties with whom the firm does not have a direct business relationship .

Simplified due diligence (SDD)

20.8. Firms should use the information they have thanks to the relationship-based nature of corporate finance activity, the scale of the transactions, and the need to assess credit risk and reputational risk posed by corporate finance arrangements also for SDD purposes.

20.9. Where firms are dealing with intermediaries who maintain accounts for the primary benefit of their underlying customers, firms should apply sectoral guideline 16.

A1

Annex: Customers that are NPOs

1. When assessing the risk profile of a customer or prospective customer that is an NPO for the first time, firms should ensure that they obtain a good understanding of the NPO's governance, how it is funded, its activities, where it operates and who its beneficiaries are. Not all NPOs are exposed in a similar way to ML/TF risk, and firms should take risk-sensitive measures to understand:

   a) who controls the customer and who its beneficial owners are. As part of this, firms should identify the NPO's trustees or equivalent, its governing body and any other individual who has control or influence over the NPO. For this purpose, firms should refer to information such as the legal status of the NPO, a description of the NPO's governance set-up and/or a list of the legal representative(s).

   b) how the NPO is funded (private donations, government funds, etc.). For this purpose, firms should refer to information about the donor base, funding sources and fundraising methods, such as annual reports and financial statements.

   c) what the objectives of the customer's operations are. For this purpose, firms should refer to information such as the customer's mission statement, a list of its programmes and associated budgets, activities, and services delivered.

   d) which categories of beneficiaries benefit from the customer's activities (for example, refugees, legal entities that receive assistance through the services of the NPO or similar). Documentation gathered for this purpose may include mission statements or campaign-related documents.

   e) what transactions the NPO is likely to request, based on its objectives and activity profile, including payment of staff or providers posted abroad, and the expected frequency, size, and geographical destination of such transactions. For this purpose, firms should refer to information such as organisational charts, explanations of the organisational structure of the NPO, a list of jurisdictions where the staff is paid and the number of employees to be paid in each of them.

   f) where the NPO conducts its programmes and/or operations, in particular whether the NPO conducts its activities only at domestic level, or in other jurisdictions associated with higher ML/TF risks and in high-risk third countries. For this purpose, firms should refer to information such as a list of all programmes, activities and services delivered by the NPO, as well as a list of geographical locations served, including its headquarters and operational areas. Firms should also assess, for the purposes of Guideline 8, whether the NPO's transactions are likely to involve the execution of payments with a third-country institution.

Risk factors

2. When identifying the risk associated with customers that are NPOs, firms should consider at

least the following risk factors and assess them on a risk-sensitive basis:

Governance and exertion of control

a) Does the NPO have a legal status under national law or the national law of another Member State? Is there any documentation that sets out its modalities of governance and identifies the NPO's trustees, members of the governing body or any other individuals who exert control over the NPO?

b) Does the legal structure of the NPO require, for its set up, the demonstration of the management capability of its treasurer or managers?

c) Does the legal structure of the NPO require the annual disclosure of financial statements?

Reputation/adverse media findings

d) To what extent is it difficult for firms to establish the good reputation of the NPO and its managers? Is there a good reason why this may be difficult, for example because the NPO has been established only recently, for instance in the last 12 months?

e) Has the NPO been linked by relevant, reliable and independent sources to extremism, extremist propaganda or terrorist sympathies and activities?

f) Has the NPO been involved in misconduct or criminal activities, including ML/TF-related cases, according to relevant, reliable and independent sources?

Funding methods

g) Is the NPO's funding transparent and accountable or difficult to trace? Does it publicly document its funding sources and are these subject to external audits?

h) Do the NPO's funding methods carry ML/TF risks? Does it rely entirely or largely on cash donations, crypto assets or crowdfunding? Or are the NPO's sources of funds channelled through the payments system?

i) Is the NPO funded partly or largely by private donors or donors from jurisdictions associated with higher ML/TF risks or high-risk third countries identified as having strategic deficiencies in their AML/CFT regime?

Operations in jurisdictions associated with higher ML/TF risks and high-risk third countries

j) Does the NPO operate or deliver assistance in jurisdictions associated with higher ML/TF risks (as assessed based on risk factors presented in Title I of these guidelines) or in high-risk third countries (as identified by the Commission pursuant to Article 9(2) of Directive (EU) 2015/849) or in conflict zones?

k) In such situations, does the NPO rely on third parties or intermediaries to perform its activities and is it able to explain the nature of the discharge? In this context, is the NPO able to monitor and have adequate oversight of the discharge by these third parties?

l) Is the business relationship with the NPO likely to involve the execution of transactions with a respondent institution located in jurisdictions associated with higher ML/TF risks or in high-risk third countries?

3. Firms should also consider at least the following factors that may contribute to reducing risks:

a) The roles and responsibilities of the NPO's governing body and its managers are clearly documented.

b) The NPO is legally required to annually disclose its financial statements or to issue an annual report that identifies the sources of funds, the main purpose of the NPO's activities and the categories of beneficiaries of its programmes.

c) The NPO can demonstrate it is or has been subject to independent reviews or external audits.

d) The NPO has a good public reputation according to relevant, reliable and independent sources.

e) The NPO receives fundings from governments, supranational or international organisations that are not associated with high-risk third countries or with jurisdictions with higher ML/TF risks, and the source of its funds can be clearly established.

f) The NPO does not have any links with high-risk third countries, or if it has, the NPO can demonstrate that it has taken appropriate steps to mitigate the ML/TF risks (for instance, with the designation of staff responsible for AML/CFT compliance or the design of procedures to identify the NPO's categories of beneficiaries and assess the ML/TF risks associated therewith).

g) The NPO's activities and beneficiaries do not expose it to higher ML/TF risks.

h) The NPO only delivers assistance and support to individuals through direct material help, such as providing IT equipment or medical devices.

4. In the event the NPO is conducting activities in jurisdictions subject to EU or UN sanctions, firms should establish whether the NPO benefits from any provisions related to humanitarian aid and derogations in EU/UN financial sanctions regimes, such as humanitarian exemptions or derogations. When deciding how to service these customers and in accordance with their own asset freezing obligations, firms should obtain evidence that provide reasonable assurance that the NPO conducts its activities in these jurisdictions in line with the exemptions provided in the regime, or that it benefits from a derogation granted by a relevant competent authority.

5. For initial screening purposes and throughout the business relationship once it is established, firms should take the steps necessary to understand how the NPO operates and conducts its operations. Firms that are likely to have NPO customers, for example because they provide money transfer services or current account services, should consider establishing a dedicated contact point for this specific category of customers to have a good understanding of the way the sector is set up and operates.