JOINT COMMITTEE OF THE EUROPEAN SUPERVISORY AUTHORITIES

JC 2017 37

26/06/2017

Final Guidelines

Joint Guidelines under Articles 17 and 18(4) of Directive (EU) 2015/849 on simplified and enhanced 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 Risk Factors Guidelines

Contents

1. Executive summary

On 26 June 2015, Directive (EU) 2015/849 on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing (Directive (EU) 2015/849) entered into force. This Directive aims, inter alia, to bring European Union legislation in line with the International Standards on Combating Money Laundering and the Financing of Terrorism and Proliferation that the Financial Action Task Force (FATF), an international anti-money laundering standard setter, adopted in 2012.

In line with the FATF's standards, Directive (EU) 2015/849 puts the risk-based approach at the centre of the European Union's anti-money laundering (AML) and countering financing of terrorism (CFT) regime. It recognises that the risk of money laundering and terrorist financing (ML/TF) can vary and that Member States, competent authorities, and credit and financial institutions within its scope ('firms') have to take steps to identify and assess that risk with a view to deciding how best to manage it.

Articles 17 and 18(4) of Directive (EU) 2015/849 require the European Supervisory Authorities (ESAs) to issue guidelines to support firms with this task and to assist competent authorities when assessing the adequacy of firms' application of simplified and enhanced customer due diligence measures. The aim is to promote the development of a common understanding, by firms and competent authorities across the EU, of what the risk-based approach to AML/CFT entails and how it should be applied.

These guidelines set out factors firms should consider when assessing the ML/TF risk associated with a business relationship or occasional transaction. They also set out how firms can adjust the extent of their customer due diligence (CDD) measures in a way that is commensurate to the ML/TF risk they have identified. The factors and measures described in these guidelines are not exhaustive and firms should consider other factors and measures as appropriate.

These guidelines are divided into two parts:

- Title II is general and applies to all firms. It is designed to equip firms with the tools they need to make informed, risk-based decisions when identifying, assessing and managing the ML/TF risk associated with individual business relationships or occasional transactions.

- Title III is sector-specific and complements the general guidance in Title II. It sets out risk factors that are of particular importance in certain sectors and provides guidance on the risk-sensitive application of CDD measures by firms in those sectors.

These guidelines will help firms identify, assess and manage the ML/TF risk associated with individual business relationships and occasional transactions in a risk-based, proportionate and effective way. They also clarify how competent authorities in the EU expect firms to discharge their obligations in this field.

Neither these guidelines nor the Directive's risk-based approach require firms to refuse to enter into, or terminate, business relationships with entire categories of customers that are associated with higher ML/TF risk.

The ESAs publicly consulted on a version of these guidelines between 22 October 2015 and 22 January 2016. Respondents welcomed the draft guidelines and considered that they would support the development of an effective risk-based approach to AML/CFT across the EU. Some respondents raised concerns about the ability of national competent authorities to apply these guidelines in a consistent manner, stressed the need for the guidelines to be consistent with international AML/CFT standards and asked for clarification regarding the interaction of these guidelines with other provisions in Union law. These concerns have been addressed in these guidelines as appropriate.

These guidelines will apply by 26 June 2018.

Next steps

The ESAs will keep these guidelines under review and update them as appropriate. The first update is likely to occur once amendments to Directive (EU) 2015/849 have been agreed. The ESAs will consult on any changes made to the substance of these guidelines.

2. Background and rationale

On 26 June 2015, Directive (EU) 2015/849 on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing (Directive (EU) 2015/849) entered into force. This Directive aims, inter alia, to bring European Union legislation in line with the International Standards on Combating Money Laundering and the Financing of Terrorism and Proliferation that the FATF, an international AML/CFT standard setter, adopted in 2012.

In line with the FATF's standards, Directive (EU) 2015/849 puts the risk-based approach at the centre of European Union's AML/CFT regime. It recognises that the risk of ML/TF can vary and that Member States, competent authorities and obliged entities have to take steps to identify and assess that risk with a view to deciding how best to manage it.

For obliged entities, CDD is central to this process, for both risk assessment and risk management purposes. CDD means:

- identifying the customer and verifying the customer's identity on the basis of documents, data or information obtained from a reliable and independent source;
- identifying the customer's beneficial owner and taking reasonable measures to verify their identity so that the obliged entity is satisfied that it knows who the beneficial owner is;
- assessing and, as appropriate, obtaining information on the purpose and intended nature of the business relationship; and
- conducting ongoing monitoring of the business relationship. This includes transaction monitoring and keeping the underlying information up to date.[1]

Directive (EU) 2015/849 provides that obliged entities can determine the extent of these measures on a risk-sensitive basis. It also provides that where the risk associated with the business relationship or occasional transaction is low, Member States may allow obliged entities to apply simplified customer due diligence (SDD) measures instead. Conversely, where the risk associated with the business relationship or occasional transaction is increased, obliged entities must apply enhanced customer due diligence (EDD) measures. However, the Directive does not set out in detail how obliged entities should assess the risk associated with a business relationship or transaction, nor does it set out exactly what SDD and EDD measures entail.

The Directive therefore requires the ESAs to issue guidelines to competent authorities and firms on 'the risk factors to be taken into consideration and/or the measures to be taken' in situations

[1] Article 13(1) of Directive (EU) 2015/849.

where SDD or EDD measures are appropriate. These guidelines have to be adopted within two years of the Directive entering into force, that is, no later than 26 June 2017.

These guidelines will support the development of a common understanding, by firms and competent authorities across the EU, of what the risk-based approach to AML/CFT entails and how it should be applied. They will help firms identify, assess and manage the ML/TF risk associated with individual business relationships and occasional transactions in a risk-based, proportionate and effective way.

Neither these guidelines nor the Directive's risk-based approach require the wholesale exiting of entire categories of customers irrespective of the ML/TF risk associated with individual business relationships or occasional transactions.

Countering the financing of terrorism

Many of the CFT measures firms have in place will overlap with their AML measures. These may cover, for example, risk assessment, CDD checks, transaction monitoring, escalation of suspicions and liaison with the authorities. The guidance provided in these guidelines therefore applies to CFT as it does to AML, even where this is not explicitly mentioned.

There are, however, key differences between preventing money laundering and countering the finance of terrorism: the money launderer seeks to disguise the origins of illicit funds, while, in contrast, a person funding terrorism may also use legitimately held funds to pursue illegal aims. Firms should bear this in mind when assessing the risks posed to the firm by those funding terrorism.

A firm's steps to counter the financing of terrorism will include its compliance with financial sanctions directed at people or organisations sanctioned for reasons related to terrorism. The European financial sanctions regime is not covered by Directive (EU) 2015/849 and compliance with this regime is not subject to a risk-based approach. It therefore falls outside the scope of these guidelines.

3. Joint guidelines under Articles 17 and 18(4) of Directive (EU) 2015/849 on simplified and enhanced 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 Risk Factors Guidelines)

Status of these joint guidelines

This document contains joint guidelines issued pursuant to Articles 16 and 56(1) of 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; Regulation (EU) No 1094/2010 establishing a European Supervisory Authority (European Insurance and Occupational Pensions Authority); and Regulation (EU) No 1095/2010 establishing a European Supervisory Authority (European Securities and Markets Authority) (the European Supervisory Authorities (ESAs) Regulations). In accordance with Article 16(3) of the ESAs Regulations, competent authorities and financial institutions must make every effort to comply with the guidelines.

Joint guidelines set out the ESAs' 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 to whom the joint guidelines apply should comply by incorporating them into their supervisory practices as appropriate (e.g. by amending their legal framework or their supervisory processes), including where the joint guidelines are directed primarily at institutions.

Reporting requirements

In accordance with Article 16(3) of the ESAs Regulations, competent authorities must notify the relevant ESA of whether they comply or intend to comply with these joint guidelines, or otherwise of reasons for non-compliance, by 26 August 2017. In the absence of any notification by this deadline, competent authorities will be considered by the relevant ESA to be non-compliant. Notifications should be sent to [compliance@eba.europa.eu, compliance@eiopa.europa.eu and compliance@esma.europa.eu] with the reference 'JC/GL/2017/34'. A template for notifications is available on the ESAs' websites. Notifications should be submitted by persons with appropriate authority to report compliance on behalf of their competent authorities.

Notifications will be published on the ESAs' websites, in line with Article 16(3).

Title I – Subject matter, scope and definitions

Subject matter

1. These guidelines set out factors firms should consider when assessing the money laundering and terrorist financing (ML/TF) risk associated with a business relationship or occasional transaction. 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.

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

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

Scope

4. 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.

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

6. 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.

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

Definitions

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

    - 'Competent authorities' means the authorities competent for ensuring firms' compliance with the requirements of Directive (EU) 2015/849 as transposed by national legislation.[2]

[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.

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

- 'jurisdictions associated with higher ML/TF risk' means countries that, based on an assessment of the risk factors set out in Title II of these guidelines, present a higher ML/TF risk. This term includes, but is not limited to, 'high-risk third countries' identified as having strategic deficiencies in their AML/CFT regime, which pose a significant threat to the Union's financial system (Article 9 of Directive (EU) 2015/849).

- '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.

- '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.

- 'Risk' means the impact and likelihood of ML/TF taking place. Risk refers to inherent risk, that is, the level of risk that exists before mitigation. It does not refer to residual risk, that is, the level of risk that remains after mitigation.

- '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.

- '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.

- 'Source of funds' means the origin of the funds involved in a business relationship or 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.

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

Title II – Assessing and managing risk: general

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

10. Firms' approach to assessing and managing the ML/TF risk associated with business relationships and occasional transactions should include the following:

- Business-wide risk assessments.

  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. To that end, and in line with Article 8 of Directive (EU) 2015/849, firms should identify and assess 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. The steps firms take to identify and assess ML/TF risk across their business must be proportionate to the nature and size of each firm. Firms that do not offer complex products or services and that have limited or no international exposure may not need an overly complex or sophisticated risk assessment.

- Customer due diligence.

  Firms should use the findings from their business-wide risk assessment to inform their decision on the appropriate level and type of CDD that they will apply to individual business relationships and occasional transactions.

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

  i. identify the customer and, where applicable, the customer's beneficial owner or legal representatives;

  ii. 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

  iii. establish the purpose and intended nature of the business relationship.

  Firms should adjust the extent of initial CDD measures on a risk-sensitive basis. Where the risk associated with a business relationship is 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 increased, firms must apply enhanced customer due diligence measures (EDD).

- Obtaining a holistic view.

Firms should gather sufficient information to be satisfied that they have identified all relevant risk factors, including, where necessary, by applying 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. Firms should note that the risk factors listed in these guidelines are not exhaustive, and that there is no expectation that firms will consider all risk factors in all cases.

- Monitoring and review.

  Firms must keep their risk assessment up to date and under review.[3] Firms must monitor transactions to ensure that they are in line with the customer's risk profile and business and, where necessary, examine the source of funds, to detect possible ML/TF. They must also keep 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.[4]

Risk assessments: methodology and risk factors

11. A risk assessment should consist of two distinct but related steps:

    a) the identification of ML/TF risk; and

    b) the assessment of ML/TF risk.

Identifying ML/TF risk

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

13. 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.

Sources of information

14. Where possible, information about these ML/TF risk factors should come from a variety of sources, whether these are accessed individually or through commercially available tools or databases that pool information from several sources. Firms should determine the type and numbers of sources on a risk-sensitive basis.

[3] Article 8(2) of Directive (EU) 2015/849.

[4] Article 13(1)(d) of Directive (EU) 2015/849.

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

- the European Commission's supranational risk assessment;
- information from government, such as the government's national risk assessments, policy statements and alerts, and explanatory memorandums to relevant legislation;
- information from regulators, such as guidance and the reasoning set out in regulatory fines;
- information from Financial Intelligence Units (FIUs) and law enforcement agencies, such as threat reports, alerts and typologies; and
- information obtained as part of the initial CDD process.

16. Other sources of information firms may consider in this context may include, among others:

- the firm's own knowledge and professional expertise;
- information from industry bodies, such as typologies and emerging risks;
- information from civil society, such as corruption indices and country reports;
- information from international standard-setting bodies such as mutual evaluation reports or legally non-binding blacklists;
- information from credible and reliable open sources, such as reports in reputable newspapers;
- information from credible and reliable commercial organisations, such as risk and intelligence reports; and
- information from statistical organisations and academia.

Risk factors

17. 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. Firms should take a holistic view of the risk associated with the situation and 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.

Customer risk factors

18. When identifying the risk associated with their customers, including their customers' beneficial owners,[5] 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.

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

- 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?

- 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?

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

- Where the customer is a legal person or a legal arrangement, what is the purpose of their establishment? For example, what is the nature of their business?

- 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.

- 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?

- Is the customer a legal person subject to enforceable disclosure requirements that ensure that reliable information about the customer's beneficial owner is publicly

[5] For guidance on risk factors associated with beneficiaries of life insurance policies, please refer to Title III, Chapter 7.

available, for example public companies listed on stock exchanges that make such disclosure a condition for listing?

- 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?

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

- 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?

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

- 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.

- 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?

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

- 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?

21. The following risk factors may be relevant when considering the risk associated with a customer's or beneficial owner's nature and behaviour; 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:

- Does the customer have legitimate reasons for being unable to provide robust

evidence of their identity, perhaps because they are an asylum seeker?[6]

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

- 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?

- 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?

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

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

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

- Does the customer request transactions that are complex, unusually or unexpectedly large or have an unusual or unexpected pattern without an apparent economic or lawful purpose or 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?

- 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?

- 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?

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

- 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

[6] The EBA has issued an 'Opinion on the application of Customer Due Diligence Measures to customers who are asylum seekers from higher risk third countries or territories', see https://eba.europa.eu/documents/10180/1359456/EBA-Op-2016-07+%28Opinion+on+Customer+Due+Diligence+on+Asylum+Seekers%29.pdf.

credit institutions can comply with their AML/CFT obligations.[7]

- Is the customer a non-profit organisation whose activities could be abused for terrorist financing purposes?

Countries and geographical areas

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

    a) the jurisdictions in which the customer and beneficial owner are based;

    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 links.

23. Firms should note that the nature and purpose of the business relationship will often determine the relative importance of individual country and geographical risk factors (see also paragraphs 36-38). For example:

    - 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.

    - 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.

    - 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.

    - Where the customer is a legal vehicle or trust, 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 standards.

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

    - 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? Where firms

[7] See, in particular, Articles 1(7) and 16(4) of Directive 2014/92/EU.

deal with natural or legal persons resident or established in third countries that the Commission has identified as presenting a high ML/TF risk, firms must always apply EDD measures.[8]

- 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.

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.

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

- 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 or that groups committing terrorist offences are known to be operating in the country or territory?

- 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 ?

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

- 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

[8] Article 18(1) of Directive (EU) 2015/849.

Standard; assessments of compliance with FATF Recommendations 9, 24 and 25 and Immediate Outcomes 2 and 5 by the FATF or FSRBs; and IMF assessments (e.g. IMF staff assessments of offshore financial centres).

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

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

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

- 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 perceptions indices; OECD country reports on the implementation of the OECD's anti-bribery convention; and the United Nations Office on Drugs and Crime World Drug Report.

- 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

28. 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.

29. Risk factors that may be relevant when considering the risk associated with a product, service or transaction's transparency include:

- 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.

- 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?

30. Risk factors that may be relevant when considering the risk associated with a product, service or transaction's complexity include:

- To what extent is the transaction complex 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?

- 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?

- 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?

31. Risk factors that may be relevant when considering the risk associated with a product, service or transaction's value or size include:

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

- 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

32. 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.

33. 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:

- Is the customer physically present for identification purposes? If they are not, has the firm used a reliable form of non-face-to-face CDD? Has it taken steps to prevent impersonation or identity fraud?

- Has the customer been introduced by another part of the same financial group and, if so, to what extent can the firm rely on this introduction as reassurance that the

customer will not expose the firm to excessive ML/TF risk? What has the firm 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?

- Has the customer been introduced by a third party, for example a bank that is not part of the same group, and is the third party a financial institution or is its main business activity unrelated to financial service provision? What has the firm done to be satisfied that:

  i. the third party applies CDD measures and keeps records to EEA standards and that it is supervised for compliance with comparable AML/CFT obligations in line with Article 26 of Directive (EU) 2015/849;

  ii. the third party will provide, immediately upon request, relevant copies of identification and verification data, inter alia in line with Article 27 of Directive (EU) 2015/849; and

  iii. the quality of the third party's CDD measures is such that it can be relied upon?

- Has the customer been introduced through a tied agent, that is, without direct firm contact? To what extent can the firm be satisfied that the agent has obtained enough information so that the firm knows its customer and the level of risk associated with the business relationship?

- If independent or tied agents are used, to what extent are they involved on an ongoing basis in the conduct of business? How does this affect the firm's knowledge of the customer and ongoing risk management?

- Where a firm uses an intermediary:

  i. Are they a regulated person subject to AML obligations that are consistent with those of Directive (EU) 2015/849?

  ii. Are they subject to effective AML supervision? Are there any indications that the intermediary's level of compliance with applicable AML legislation or regulation is inadequate, for example has the intermediary been sanctioned for breaches of AML/CFT obligations?

  iii. Are they based in a jurisdiction associated with higher ML/TF risk? Where a third party is based in a high-risk third country that the Commission has identified as having strategic deficiencies, firms must not rely on that intermediary. 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.[9]

Assessing ML/TF risk

34. 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 or occasional transaction.

35. As part of this assessment, firms may decide to weigh factors differently depending on their relative importance.

Weighting risk factors

36. When weighting risk factors, firms should make an informed judgement about the relevance of different risk factors in the context of a business relationship or occasional transaction. 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.

37. 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:

- weighting is not unduly influenced by just one factor;
- economic or profit considerations do not influence the risk rating;
- weighting does not lead to a situation where it is impossible for any business relationship to be classified as high risk;
- 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
- 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.

38. 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 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.

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

Categorising business relationships and occasional transactions

39. Following its risk assessment, a firm should categorise its business relationships and occasional transactions according to the perceived level of ML/TF risk.

40. 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.

Risk management: simplified and enhanced customer due diligence

41. A firm's risk assessment should help it identify where it should focus its AML/CFT risk management efforts, both at customer take-on and for the duration of the business relationship.

42. As part of this, 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 these measures on a risk-sensitive basis. CDD measures should help firms better understand the risk associated with individual business relationships or occasional transactions.

43. Article 13(4) of Directive (EU) 2015/849 requires firms to be able to demonstrate to their competent authority that the CDD measures they have applied are commensurate to the ML/TF risks.

Simplified customer due diligence

44. 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.

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

- adjusting 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.

- 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 centre gift card.

- 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 in relation to 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.

- 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 customer looking 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.

- 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.

46. Title III lists additional SDD measures that may be of particular relevance in different sectors.

47. 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.

48. 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.[10] Equally, where specific high-risk scenarios apply and there is an obligation to conduct EDD, SDD must not be applied.

Enhanced customer due diligence

49. Firms must apply EDD measures in higher risk situations to manage and mitigate those risks appropriately.[11] EDD measures cannot be substituted for regular CDD measures but must be applied in addition to regular CDD measures.

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

    i. where the customer, or the customer's beneficial owner, is a PEP;[12]

    ii. where a firm enters into a correspondent relationship with a respondent institution from a non-EEA state;[13]

    iii. where a firm deals with natural persons or legal entities established in high-risk third countries;[14] and

    iv. all complex and unusually large transactions, or unusual patterns of transactions, that have no obvious economic or lawful purpose.[15]

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

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

    ii. with respect to correspondent relationships with respondents from third countries; and

[10] Article 11(e) and (f) and Article 15(2) of Directive (EU) 2015/849.
[11] Articles 18-24 of Directive (EU) 2015/849.
[12] Articles 20-24 of Directive (EU) 2015/849.
[13] Article 19 of Directive (EU) 2015/849.
[14] Article 18(1) of Directive (EU) 2015/849.
[15] Article 18(2) of Directive (EU) 2015/849.

iii. with respect to all complex and unusually large transactions, or unusual patterns of transactions, that have no obvious 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

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

- 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.

- 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.

  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.

- 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.

53. 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.[16]

Correspondent relationships

54. Firms must take specific EDD measures where they have a cross-border correspondent

[16] Article 20(b) of Directive (EU) 2015/849.

relationship with a respondent who is based in a third country.[17] Firms must apply all of these measures and should adjust the extent of these measures on a risk-sensitive basis.

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

Unusual transactions

56. Firms should put in place adequate policies and procedures to detect unusual transactions or patterns of transactions. Where a firm detects transactions that are unusual because:

- 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;
- 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
- 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, it must apply EDD measures.

57. These EDD measures should be sufficient to help the firm determine whether these transactions give rise to suspicion and must at least include:

- 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
- 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.

High-risk third countries and other high-risk situations

58. When dealing with natural persons or legal persons established or residing in a high-risk third country identified by the Commission[18] and 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

[17] Article 19 of Directive (EU) 2015/849.

[18] Article 9 of Directive (EU) 2015/849.

reason why an occasional transaction or a business relationship was classified as high risk.

59. 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.

60. EDD measures firms should apply may include:

- Increasing the quantity of information obtained for CDD purposes:

  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.

- 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.

- 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.

61. Title III lists additional EDD measures that may be of particular relevance in different sectors.

Other considerations

62. 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.

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

64. 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 and review

Risk assessment

65. Firms should keep their assessments of the ML/TF risk associated with individual business relationships and occasional transactions as well as of the underlying factors under review to ensure their assessment of ML/TF risk remains up to date and relevant. Firms should assess information obtained as part of their ongoing monitoring of a business relationship and consider whether this affects the risk assessment.

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

67. Examples of systems and controls firms should put in place to identify emerging risks include:

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

- Processes to ensure that the firm regularly reviews relevant information sources such as those specified in paragraphs 15 and 16 of these guidelines. This should involve, in particular:

  i. regularly reviewing media reports that are relevant to the sectors or jurisdictions in which the firm is active;

  ii. regularly reviewing law enforcement alerts and reports;

  iii. ensuring that the firm becomes aware of changes to terror alerts and sanctions regimes as soon as they occur, for example by regularly reviewing terror alerts and looking for sanctions regime updates; and

  iv. regularly reviewing thematic reviews and similar publications issued by competent authorities.

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

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

- Establishing a culture of information sharing within the firm and strong company ethics.

68. Examples of systems and controls firms should put in place to ensure their individual and business-wide risk assessments remains up to date may include:

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

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

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

Systems and controls

70. Firms should take steps to ensure that their risk management systems and controls, in particular those relating to the application of the right level of CDD measures, are effective and proportionate.

Record keeping

71. Firms should record and document their risk assessments of business relationships, as well as any changes made to risk assessments as part of their reviews and monitoring, to ensure that they can demonstrate to the competent authorities that their risk assessments and associated risk management measures are adequate.

Title III – Sector-specific guidelines

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

73. The risk factors described in each chapter of Title III 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.

74. Each chapter in Title III 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.

Chapter 1: Sectoral guidelines for correspondent banks

75. This chapter 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.

76. 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.

77. Banks should consider the following risk factors and measures alongside those set out in Title II of these guidelines.

Risk factors

Product, service and transaction risk factors

78. The following factors may contribute to increasing risk:

- 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.

- 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.

- 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.

79. The following factors may contribute to reducing risk:

- The relationship is limited to a SWIFT 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.

- 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.

- 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

80. The following factors may contribute to increasing risk:

- 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.
- The respondent is not subject to adequate AML/CFT supervision.
- 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.
- 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.
- 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.
- The history of the business relationship with the respondent gives rise to concern, for example because the amount of transactions are not in line with what the correspondent would expect based on its knowledge of the nature and size of the respondent.

81. The following factors may contribute to reducing risk:

The correspondent is satisfied that:

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

82. The following factors may contribute to increasing risk:

- The respondent is based in a jurisdiction associated with higher ML/TF risk. Firms

should pay particular attention to those jurisdictions

- with significant levels of corruption and/or other predicate offences to money laundering;
- without adequate capacity of the legal and judicial system effectively to prosecute those offences; or
- without effective AML/CFT supervision.[19]

- The respondent conducts significant business with customers based in a jurisdiction associated with higher ML/TF risk.
- The respondent's parent is headquartered or is incorporated in a jurisdiction associated with higher ML/TF risk.

83. The following factors may contribute to reducing risk:

- The respondent is based in an EEA member country.
- 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

84. All correspondents must carry out CDD on the respondent, who is the correspondent's customer, on a risk-sensitive basis.[20] This means that correspondents must:

- 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.

[19] See also Title II, paragraphs 22-27.

[20] Article 13 of Directive (EU) 2015/849.

- 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).

- 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. Due to the nature of correspondent banking, post-execution monitoring is the norm.

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

85. Correspondents must also establish that the respondent does not permit its accounts to be used by a shell bank,[21] in 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.

86. In cases of cross-border correspondent relationships with respondent institutions from third countries, Article 19 of Directive (EU) 2015/849 requires that the correspondent also apply specific EDD measures in addition to the CDD measures set out in Article 13 of Directive (EU) 2015/849.

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

88. Correspondents should bear in mind 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

89. Where the respondent is based in a third country, Article 19 of Directive (EU) 2015/849 requires correspondents to apply specific EDD measures in addition to the CDD measures set out in Article 13 of Directive (EU) 2015/849.

90. Correspondents must apply each of these EDD measures to respondents based in a non-

[21] Article 3(17) of Directive (EU) 2015/849.

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 policies and procedures are, or have recently been deemed, inadequate, then the assessment of the respondent's AML controls may not necessarily have to be carried out in full detail.

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

92. Article 19 of Directive (EU) 2015/849 requires correspondents to take risk-sensitive measures to:

- 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 and the type of activities that the respondent will transact through the correspondent account.

- 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.

- 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.

- Obtain approval from senior management, as defined in Article 3(12) of Directive (EU) 2015/849, before establishing new correspondent relationships. The approving senior manager should not be the officer sponsoring the relationship and the higher the risk associated with the relationship, the more senior the approving senior manager should be. Correspondents should keep senior management informed of high-risk correspondent banking relationships and the steps the correspondent takes to manage that risk effectively.

- Document the responsibilities of each institution. This may be part of the correspondent's standard terms and conditions but correspondents should set out, in writing, how and by whom the correspondent banking facility can be used (e.g. if it can be used by other banks through their relationship with the respondent) and what the

respondent's AML/CFT responsibilities are. Where the risk associated with the relationship is high, it may be appropriate for the correspondent to satisfy itself that the respondent complies with its responsibilities under this agreement, for example through ex post transaction monitoring.

- 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

93. 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.

94. 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).

Chapter 2: Sectoral guidelines for retail banks

95. 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.

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

97. Banks should consider the following risk factors and measures alongside those set out in Title II of these guidelines.

Risk factors

Product, service and transaction risk factors

98. The following factors may contribute to increasing risk:

- the product's features favour anonymity;
- 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;
- the product places no restrictions on turnover, cross-border transactions or similar product features;
- new products and new business practices, including new delivery mechanisms, and the use of new or developing technologies for both new and existing products where these are not yet well understood;
- 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;
- an unusually high volume or large value of transactions.

99. The following factors may contribute to reducing risk:

- 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.

- 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.

- 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.

- There is no overpayment facility.

Customer risk factors

100. The following factors may contribute to increasing risk:

- 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.[22]

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.

- 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.

101. The following factor may contribute to reducing risk:

- 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[23]

102. The following factors may contribute to increasing risk:

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

- 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.

[22] 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 .

[23] See also Title II.

103. The following factor may contribute to reducing risk:

- 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

104. The following factors may contribute to increasing risk:

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

- 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;

- new delivery channels that have not been tested yet.

105. The following factor may contribute to reducing risk:

- 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

106. 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 II. The use of automated IT systems should never be considered a substitute for staff vigilance.

Enhanced customer due diligence

107. Where the risk associated with a business relationship or occasional transaction is increased, banks must apply EDD measures.[24] These may include:

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

- 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.

[24] Article 18 of Directive (EU) 2015/849.

- 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.

- Increasing the frequency of transaction monitoring.

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

Simplified customer due diligence

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

- 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;

- 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;

- 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;

- 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;

- 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

109. 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.

110. Where there are indications that the risk associated with the business relationship is high, banks must apply EDD measures as appropriate.[25]

111. 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:

- 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.

- 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.

- 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;

- 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

- 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.

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

[25] Articles 13(1) and 18(1) of Directive (EU) 2015/849.

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

Chapter 3: Sectoral guidelines for electronic money issuers

113. This chapter 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[26] (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.[27]

114. Firms that issue e-money should consider the following risk factors and measures alongside those set out in Title II of these guidelines. The sectoral guidelines for money remitters in Title III, Chapter 4, may also be relevant in this context.

Risk factors

Product risk factors

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

- thresholds;
- the funding method; and
- utility and negotiability.

116. The following factors may contribute to increasing risk:

- Thresholds: the product allows
  - i. high-value or unlimited-value payments, loading or redemption, including cash withdrawal;
  - ii. high-value payments, loading or redemption, including cash withdrawal;
  - iii. high or unlimited amount of funds to be stored on the e-money product/account.
- 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.

[26] Article 2(2) of Directive 2009/110/EC.
[27] Article 3(4) of Directive 2009/110/EC.

- 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.

117. The following factors may contribute to reducing risk:

- 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.

- 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;

- 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

118. The following factors may contribute to increasing risk:

- 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.

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

- 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).

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

- 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.

119. The following factor may contribute to reducing risk:

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

Distribution channel risk factors

120. The following factors may contribute to increasing risk:

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

- 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; and

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

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

Country or geographical risk factors;[28]

121. The following factors may contribute to increasing risk:

- The payee is located in, or the product receives funds from sources 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.

Measures

122. 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.

123. 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.

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

- 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;

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

- 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;

- 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.

[28] See Title II, paragraphs 22-27.

Enhanced customer due diligence

125. Examples of EDD measures firms should apply in a high-risk situation include:

- obtaining additional customer information during identification, such as the source of funds;
- 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;
- 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;
- 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;
- applying identity fraud checks to ensure that the customer is who they claim to be;
- applying enhanced monitoring to the customer relationship and individual transactions;
- establishing the source and/or the destination of funds.

Simplified customer due diligence

126. 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.

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

- 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 250 where the product is not reloadable or can be used in other jurisdictions or for cross-border transactions or EUR 500 where permitted by national legislation (in this case, the product can be used only domestically);
- 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;
- verifying identity on the basis of fewer sources;
- verifying identity on the basis of less reliable sources;

- using alternative methods to verify identity;

- 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;

- 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.

Chapter 4: Sectoral guidelines for money remitters

128. Money remitters are payment institutions that have been authorised in line with Directive 2007/64/EC 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.

129. 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.

130. 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.

131. Money remitters should consider the following risk factors and measures alongside those set out in Title II of these guidelines.

Risk factors

Product, service and transaction risk factors

132. The following factors may contribute to increasing risk:

- the product allows high-value or unlimited-value transactions;
- the product or service has a global reach;
- 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;
- transfers are made from one or more payers in different countries to a local payee.

133. The following factor may contribute to reducing risk:

- 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

134. The following factors may contribute to increasing risk:

- 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.

- 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.[29] 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.

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).

135. The following factors may contribute to reducing risk:

- 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

[29] 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 (Text with EEA relevance).

increased.

- 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

136. The following factors may contribute to increasing risk:

- 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.

- The distribution channel used provides a degree of anonymity.

- The service is provided entirely online without adequate safeguards.

- 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.

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

- 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.

137. The following factors may contribute to reducing risk:

- Agents are themselves regulated financial institutions.

- 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

138. The following factors may contribute to increasing risk:

- The payer or the payee is located in a jurisdiction associated with higher ML/TF risk.
- 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.

Measures

139. 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.

140. Firms should in any case put in place:

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

141. Where the risk associated with an occasional transaction or business relationship is increased, firms should apply EDD in line with Title II, 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 II.

Use of agents

142. Money remitters using agents to provide payment services should know who their agents are.[30] 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:

[30] Article 19 of Directive (EU) 2366/2015.

- 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.

- 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.

- 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.

- 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.

Chapter 5: Sectoral guidelines for wealth management

143. 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.

144. 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.

145. Firms in this sector should consider the following risk factors and measures alongside those set out in Title II of these guidelines. The sectoral guidelines in Title III, Chapters 2, 7 and 9, may also be relevant in this context.

Risk factors

Product, service and transaction risk factors

146. The following factors may contribute to increasing risk:

- customers requesting large amounts of cash or other physical stores of value such as precious metals;
- very high-value transactions;
- 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);[31]
- 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;
- 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;
- business taking place across multiple countries, particularly where it involves multiple

[31] See also Title II, paragraph 26.

providers of financial services;

- cross-border arrangements where assets are deposited or managed in another financial institution, either of the same financial group or outside of the group, particularly where the other financial institution is based in a 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

147. The following factors may contribute to increasing risk:

- Customers with income and/or wealth from high-risk sectors such as arms, the extractive industries, construction, gambling or private military contractors.
- Customers about whom credible allegations of wrongdoing have been made.
- Customers who expect unusually high levels of confidentiality or discretion.
- Customers whose spending or transactional behaviour makes it difficult to establish 'normal', or expected patterns of behaviour.
- 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.
- 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[32]

148. The following factors may contribute to increasing risk:

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

Measures

149. The staff member managing a wealth management firm's relationship with a customer (the relationship manager) should play a key role in assessing risk. The relationship

[32] See also Title II.

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, 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

150. The following EDD measures may be appropriate in high-risk situations:

- 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.

- 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 an advocate or solicitor;

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

  vi. written confirmation of inheritance signed by an advocate, solicitor, trustee or executor;

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

- Establishing the destination of funds.

- 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.

- Carrying out an independent internal review and, where appropriate, seeking senior management approval of new clients and existing clients on a risk-sensitive basis.

- Monitoring transactions on an ongoing basis, including, where necessary, reviewing each transaction as it occurs, to detect unusual or suspicious activity. This may include measures to determine whether any of the following are out of line with the business risk profile:

  i. transfers (of cash, investments or other assets);

  ii. the use of wire transfers;

  iii. significant changes in activity;

  iv. transactions involving jurisdictions associated with higher ML/TF risk.

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

- Monitoring public reports or other sources of intelligence to identify information that relates to clients or to their known associates, businesses to which they are connected, potential corporate acquisition targets or third party beneficiaries to whom the client makes payments.

- Ensuring that cash or other physical stores of value (e.g. travellers' cheques) are handled only at bank counters, and never by relationship managers.

- Ensuring that the firm is satisfied that a client's use of complex business structures such as trusts and private investment vehicles is for legitimate and genuine purposes, and that the identity of the ultimate beneficial owner is understood.

Simplified customer due diligence

151. Simplified due diligence is not appropriate in a wealth management context.

Chapter 6: Sectoral guidelines for trade finance providers

152. 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.

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

- '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 II to manage the risk associated with such transactions.

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

- 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.

154. 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 II.

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

156. The International Chamber of Commerce (ICC) has developed standards that govern the use of LCs and BCs, but these do not cover matters related to financial crime.33 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.

157. Firms in this sector should consider the following risk factors and measures alongside those set out in Title II of these guidelines. The sectoral guidelines in Title III, Chapter 1, may also be relevant in this context.

[33] Uniform Customs and Practice for Documentary Credits (UCP 600) for LCs and Uniform Rules for Collections (URC 522) for BCs.

Risk factors

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

159. 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.

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

Transaction risk factors

161. The following factors may contribute to increasing risk:

- The transaction is unusually large given what is known about a customer's previous trading activity.
- The transaction is highly structured, fragmented or complex, involving multiple parties, without apparent legitimate justification.
- Copy documents are used in situations where original documentation would be expected, without reasonable explanation.
- There are significant discrepancies in documentation, for example between the description of goods in key documents (i.e. invoices and transport documents) and actual goods shipped, to the extent that this is known.
- The type, quantity and value of goods is inconsistent with the bank's knowledge of the buyer's business.
- 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.
- The goods transacted require export licences.
- The trade documentation does not comply with applicable laws or standards.
- Unit pricing appears unusual, based on what the bank knows about the goods and trade.
- 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.

162. The following factors may contribute to reducing risk:

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

- 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

163. The following factors may contribute to increasing risk:

- 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).

- 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.

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

- The buyer uses agents or third parties.

164. The following factors may contribute to reducing risk:

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

- The customer is listed on a stock exchange with disclosure requirements similar to the EU's.

Country or geographical risk factors

165. The following factors may contribute to increasing risk:

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

- 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.

166. The following factors may contribute to reducing risk:

- The trade is within the EU/EEA.
- 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

167. 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.

168. 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, which trading routes are used, which goods are traded, who the customer does business with (buyers, suppliers, etc.), whether the customer uses agents or third parties, and, if so, where these are based. This should help banks understand who the customer is and aid the detection of unusual or suspicious transactions.

169. Where a bank is a correspondent, it must apply CDD measures to the respondent. Correspondent banks should follow the guidelines on correspondent banking in Title III, Chapter 1.

Enhanced customer due diligence

170. In higher risk situations, banks must 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.

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

- 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.
- Obtaining more information on the financial situation of the parties involved.

172. Checks on transactions may include:

- 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;

- 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;

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

173. 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.[34]

Simplified customer due diligence

174. 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.

[34] Banks routinely check documents to detect attempts to defraud the bank or its customer. They are a key part of the service provided by a bank offering trade finance. It may be possible for banks to build on these existing controls to meet their AML/CFT obligations.

Chapter 7: Sectoral guidelines for life insurance undertakings

175. 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). The 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.

176. 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.

177. 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.

178. Firms in this sector should consider the following risk factors and measures alongside those set out in Title II of these guidelines. The sectoral guidelines in Title III, Chapters 5 and 9, may also be relevant in this context. Where intermediaries are used, the delivery channel risk factors set out in Title II, paragraphs 32-33, will be relevant.

179. Intermediaries may also find these guidelines useful.

Risk factors

Product, service and transaction risk factors

180. The following factors may contribute to increasing risk:

- 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.
- Ease of access to accumulated funds, for example the product allows partial withdrawals or early surrender at any time, with limited charges or fees.
- Negotiability, for example the product can be:
  i. traded on a secondary market;

ii. used as collateral for a loan.

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

181. Factors that may contribute to reducing risk include:

The product:

- only pays out against a pre-defined event, for example death, or on a specific date, such as in the case of credit life insurance policies covering consumer and mortgage loans and paying out only on death of the insured person;
- has no surrender value;
- has no investment element;
- has no third party payment facility;
- requires that total investment is curtailed at a low value;
- is a life insurance policy where the premium is low;
- only allows small-value regular premium payments, for example no overpayment;
- 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;
- cannot be redeemed in the short or medium term, as in the case of pension schemes without an early surrender option;
- cannot be used as collateral;
- does not allow cash payments;
- has conditions that must be met to benefit from tax relief.

Customer and beneficiary risk factors

182. The following factors may contribute to increasing risk:

- 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.

- 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;[35]

     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;

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

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.

183. The following factors may contribute to reducing risk:

In the case of corporate-owned life insurance, the customer is:

- 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;
- a public company listed on a stock exchange and subject to regulatory disclosure requirements (either by stock exchange rules or through law or enforceable means) that impose requirements to ensure adequate transparency of beneficial ownership, or a majority-owned subsidiary of such a company;
- a public administration or a public enterprise from an EEA jurisdiction.

Distribution channel risk factors

184. The following factors may contribute to increasing risk:

- non-face-to-face sales, such as online, postal or telephone sales, without adequate safeguards, such as electronic signatures or electronic identification documents that comply with Regulation (EU) No 910/2014;
- long chains of intermediaries;
- an intermediary is used in unusual circumstances (e.g. unexplained geographical distance).

185. The following factors may contribute to reducing risk:

- 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.

- 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

186. The following factors may contribute to increasing risk:

- 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.

- 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.

- 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.

187. The following factors may contribute to reducing risk:

- Countries are identified by credible sources, such as mutual evaluations or detailed assessment reports, as having effective AML/CFT systems.

- Countries are identified by credible sources as having a low level of corruption and other criminal activity.

Measures

188. 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:

- obtain the name of the beneficiary where either a natural or legal person or an arrangement is identified as the beneficiary; or

- 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.

189. Firms must verify the beneficiaries' identities at the latest at the time of payout.

190. 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.

Enhanced customer due diligence

191. The following EDD measures may be appropriate in a high-risk situation:

- 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.

- 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 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.

192. 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.

193. More frequent and more in-depth monitoring of transactions may be required (including where necessary, establishing the source of funds).

Simplified customer due diligence

194. The following measures may satisfy some of the CDD requirements in low-risk situations (to the extent permitted by national legislation):

- 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.

- 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.

Chapter 8: Sectoral guidelines for investment firms

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

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

197. Firms in this sector should consider the following risk factors and measures alongside those set out in Title II of these guidelines. The sectoral guidelines in Title III, Chapter 5, may also be relevant in this context.

Risk factors

Product, service or transaction risk factors

198. The following factors may contribute to increasing risk:

- transactions are unusually large;
- third party payments are possible;
- the product or service is used for subscriptions that are quickly followed by redemption possibilities, with limited intervention by the investment manager.

Customer risk factors

199. The following factors may contribute to increasing risk:

- 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.

- The customer's nature, for example:

  i. the customer is a company or trust 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 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.

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

200. The following factors may contribute to reducing risk:

- The customer is an institutional investor whose status has been verified by an EEA government agency, for example a government-approved pensions scheme.

- The customer is a government body from an EEA jurisdiction.

- The customer is a financial institution established in an EEA jurisdiction.

Country or geographical risk factors

201. The following factors may contribute to increasing risk:

- The investor or their custodian is based in a jurisdiction associated with higher ML/TF risk.
- The funds come from a jurisdiction associated with higher ML/TF risk.

Measures

202. 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.

203. Firms should follow the EDD guidelines set out in Title II in higher risk situations. In addition, where the risk associated with a business relationship is high, firms should:

- 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;
- understand the reason for any payment or transfer to or from an unverified third party.

204. To the extent permitted by national legislation, investment managers may apply the SDD guidelines set out in Title II in low-risk situations.

Chapter 9: Sectoral guidelines for providers of investment funds

205. The provision of investment funds can involve multiple parties: 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.

206. The type and number of parties involved in the funds 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.

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

- 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.

- Alternative investment funds, such as hedge funds, real estate and private equity funds, tend to have a smaller number of investors, which can be private individuals as well as institutional investors (pension funds, funds of funds). Funds that are designed for a limited number of high-net-worth individuals, or for family offices, can have an inherently higher risk of abuse for ML/TF purposes than retail funds, since investors are more likely to be in a position to exercise control over the fund 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.

- 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.

208. This chapter is directed at:

a) investment fund managers performing activities under Article 3(2)(a) of Directive (EU) 2015/849; and

b) investment funds marketing their own shares or units, under Article 3(2)(d) of Directive (EU) 2015/849.

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.

209. For funds and fund managers, the sectoral guidelines in Title III, Chapters 1, 7 and 8, may also be relevant.

Risk factors

Product, service or transaction risk factors

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

- The fund is designed for a limited number of individuals or family offices, for example a private fund or single investor fund.
- It is possible to subscribe to the fund and then quickly redeem the investment without the investor incurring significant administrative costs.
- Units of or shares in the fund can be traded without the fund or fund manager being notified at the time of the trade and, as a result, information about the investor is divided among several subjects (as is the case with closed-ended funds traded on secondary markets).

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

- 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 paragraphs 22-27 of Title II of the guidelines.
- The subscription involves third party subscribers or payees, in particular where this is unexpected.

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

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

Customer risk factors

213. The following factors may contribute to increasing risk:

- The customer's behaviour is unusual, for example:

  i. 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.

  ii. The customer asks to repurchase or redeem an investment within a short period after the initial investment or before the payout date without a clear rationale,

in particular where this results in financial loss or payment of high transaction fees.

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. The customer transfers funds in excess of those required for the investment and asks for surplus amounts to be reimbursed.

v. 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.

vi. 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.

vii. The customer suddenly changes the settlement location without rationale, for example by changing the customer's country of residence.

viii. The customer and the beneficial owner are located in different jurisdictions and at least one of these jurisdictions is associated with higher ML/TF risk as defined in the general part of the guidelines.

ix. The beneficial owner's funds have been generated in a jurisdiction associated with higher ML/TF risk, in particular where the jurisdiction is associated with higher levels of predicate offences to ML/TF.

214. The following factors may contribute to reducing risk:

- the customer is an institutional investor whose status has been verified by an EEA government agency, for example a government-approved pensions scheme;
- the customer is a firm in an EEA country or a third country that has AML/CFT requirements that are not less robust than those required by Directive (EU) 2015/849.

Distribution channel risk factors

215. The following factors may contribute to increasing risk:

- unclear or 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;
- the distributor is located in a jurisdiction associated with higher ML/TF risk as defined in the general part of these guidelines.

216. The following factors may indicate lower risk:

- 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.

- The fund can be purchased and redeemed only through a firm, for example a financial intermediary, in an EEA country or a third country that has AML/CFT requirements that are not less robust than those required by Directive (EU) 2015/849.

Country or geographical risk factors

217. The following factors may contribute to increasing risk:

- Investors' monies have been generated in jurisdictions associated with higher ML/TF risk, in particular those associated with higher levels of predicate offences to money laundering.

- The fund or fund manager invests in sectors with higher corruption risk (e.g. the extractive industries or the arms trade) in jurisdictions identified by credible sources as having significant levels of corruption or other predicate offences to ML/TF, in particular where the fund is a single investor fund or has a limited number of investors.

Measures

218. 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 investor 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.

219. 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 the registered owner of the shares or units 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 the registered owner of the shares or units (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 the firm does not become the legal owner of the units or shares).

SDD and EDD measures to be taken in the situations described in paragraphs 219a and 219b

220. In the situations described in paragraphs 219a and 219b, examples of EDD measures a fund or fund manager should apply in high-risk situations include:

- obtaining additional customer information, such as the customer's reputation and background, before the establishment of the business relationship;
- taking additional steps to further verify the documents, data or information obtained;
- obtaining information on the source of funds and/or the source wealth of the customer and of the customer's beneficial owner;
- 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;
- increasing the frequency and intensity of transaction monitoring;
- requiring 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;
- obtaining approval from senior management at the time of the transaction when a customer uses a product or service for the first time;
- enhanced monitoring of the customer relationship and individual transactions.

221. 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.

SDD and EDD measures to be taken in situations described in paragraph 219c

222. In the situations described in paragraph 219c, 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 are 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

paragraph 112 of these guidelines, subject to the following conditions:

- 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.

- The financial intermediary is effectively supervised for compliance with these requirements.

- 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.

- 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.

- 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.

223. 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 paragraph 220 above.

SDD and EDD measures to be taken in situations described in paragraph 219d

224. In the situations described in paragraph 219d, 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.

225. 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 paragraph 222 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.

226. 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

paragraph 220 above.

Title IV – Implementation

Implementation

227. Competent authorities and firms should comply with these guidelines by 26 June 2018.

4. Accompanying documents

4.1. Impact assessment

Introduction

1. Directive (EU) 2015/849 places the risk-based approach at the centre of the Union's AML/CFT regime. It makes clear that the risk of ML/TF can vary and states that a risk-based approach helps effectively to manage that risk. What credit and financial institutions ('firms') do to understand who their customers are is central to this process.

2. Directive (EU) 2015/849 requires the ESAs to issue guidelines to competent authorities and firms on the risk factors firms should take into consideration and the measures they should take in situations where simplified or enhanced CDD would be appropriate. The aim is to promote a common understanding, by firms and competent authorities, of what the risk-based approach to AML/CFT entails and how it should be applied.

Scope and objectives

3. This impact assessment describes the policy options the ESAs considered when drafting these guidelines and sets out how these options might affect their stakeholders.

4. The ESAs considered the views of AML/CFT competent authorities, existing cost-benefit analyses and the Commission Staff's impact assessment of its proposal for a fourth Anti-Money Laundering Directive. They found that the application of these guidelines would not give rise to significant costs over and above those that firms and competent authorities would incur as a result of the underlying legal obligations set out in Directive (EU) 2015/849.

5. The ESAs therefore considered that it would not be proportionate to carry out a full, quantitative assessment of the costs and benefits arising from the application of the proposed guidelines by competent authorities and firms. Instead, this impact assessment examines, in qualitative terms, the impact that these guidelines would have if all firms and competent authorities fully complied with them. This means that the estimated net impact of the preferred options should be interpreted as the maximum impact of the full implementation of the proposed guidelines; the impact of the actual implementation of these guidelines could be less.

Baseline

6. Article 17 of Directive (EU) 2015/849 requires the ESAs to issue guidelines on the risk factors to be taken into consideration and the measures to be taken in situations where SDD measures are appropriate.

7. Article 18(4) of Directive (EU) 2015/849 requires the ESAs to issue guidelines on the risk factors to be taken into consideration and the measures to be taken in situations where

EDD measures are appropriate.

8. In both cases, the ESAs have to take specific account of the nature and size of firms' business.

9. The ESAs considered options in relation to

   - the consistency of these guidelines with international AML/CFT standards;
   - the structure of these guidelines;
   - the guidelines' addressees; and
   - the level of prescription.

Consistency with international AML/CFT standards

10. The ESAs have not issued guidelines on ML/TF risk factors or simplified and enhanced CDD so far. However, relevant guidance has been published by international standard setters, including the FATF and the Basel Committee on Banking Supervision.

Option 1

11. The ESAs' guidelines could reproduce, or simply refer to, international standards and guidance on ML/TF risk factors and simplified and enhanced CDD.

12. The advantage of this approach is that it consolidates existing guidance and makes compliance easier for firms with an international footprint.

13. The disadvantage is that existing international guidance is insufficient, by itself, to meet the requirements of Articles 17 and 18(4) of Directive (EU) 2015/849. This is because international guidance does not:

    - take into account specific measures set out in Directive (EU) 2015/849, for example in relation to certain electronic money products or high-risk third countries that have been identified by the Commission as posing significant risks to the Union's financial system;
    - cover all the financial sectors included in Directive (EU) 2015/849's scope; or
    - contain sufficient detail to ensure the consistent application of Directive (EU) 2015/849's risk-based approach.

Option 2

14. The ESAs' guidelines could be drafted in a way that is consistent with existing international standards and guidance.

15. The advantage of this approach is that it allows the ESAs to address provisions that are

specific to Directive (EU) 2015/849 and tailor their approach to those financial sectors within Directive (EU) 2015/849's scope. It also allows the drafting of the guidelines in a way that is conducive to the consistent and coherent application of the risk-based approach by firms and competent authorities across the EU.

16. The disadvantage is that there is a risk that amendments to, or new, international guidelines may not be consistent with the ESAs' guidelines. This approach would therefore mean reviewing and, where necessary, updating the guidelines periodically and whenever international standard setters reconsider their guidance and standards.

Option 3

17. The ESAs' guidelines could be drafted without regard to international standards and guidance.

18. The advantage of this approach is that it allows the ESAs to issue guidelines specific to the European context.

19. The disadvantage of this approach is that it risks exposing Member States to international censure should their approach be in breach of international standards.

Preferred option

20. Option 2 is the ESAs' preferred option because it allows firms and competent authorities to comply with international standards and guidelines while fostering the consistent and coherent application of the risk-based approach across the EU.

Structure of the guidelines

21. The ESAs have two mandates to issue guidelines on risk factors and CDD, one in relation to high-risk situations and one in relation to low-risk situations.

Option 1

22. The ESAs could issue two sets of guidelines.

23. The advantage of this approach is that this might result in two sets of short guidelines.

24. The disadvantage is that separate guidelines risk being duplicative, as it is not enough, under a risk-based approach, to consider either high-risk or low-risk factors only: firms should always consider all relevant risk factors in order to obtain a holistic view of the risk to which they are exposed and manage that risk appropriately.

Option 2

25. The ESAs could issue a single set of guidelines on both simplified and enhanced CDD.

26. The advantage of this approach is that a single set of guidelines is more conducive to

firms and competent authorities obtaining a holistic view of the risk associated with individual business relationships and occasional transactions than are separate guidelines on high and low risk.

27. The disadvantage is that these more complex guidelines may be more difficult to navigate for firms with less previous exposure to AML/CFT issues and the risk-based approach.

Preferred option

28. Option 2 is the ESAs' preferred approach as it better reflects how firms and competent authorities should implement the risk-based approach.

Addressees

29. Directive (EU) 2015/849 requires that the ESAs take account of the nature and size of firms' business.

Option 1

30. The ESAs could issue one set of guidelines for all firms.

31. The advantage of this approach is that it ensures the development of a consistent approach to the application of the risk-based approach across the entire financial services industry.

32. The disadvantage is that this approach does not take into account the diversity of Europe's financial sector and risks being unduly prescriptive, ineffective or onerous for at least some firms.

Option 2

33. The ESAs could draft guidelines for each sector.

34. The advantage of this approach is that it allows the development of guidelines in a targeted, proportionate and effective way, which takes into account the nature and size of different types of firms.

35. The disadvantage is that it does not lend itself to the development of a consistent European approach to AML/CFT.

Option 3

36. The ESAs could draft guidelines that apply to all firms and supplement these with sector-specific guidelines.

37. The advantage of this option is that it facilitates both the development of a common understanding of the risk-based approach and the drafting of targeted guidelines that take account of the specificities of firms in key sectors. This should be conducive to more consistent practices and supervisory expectations.

38. The disadvantage is that there is a risk that some firms will only have regard to the sector-specific guidelines, which are incomplete on their own. This would mean that these firms' AML/CFT systems and controls would be unlikely to be effective.

Preferred option

39. Option 3 is the ESAs' preferred option, as it benefits from the advantages associated with Options 1 and 2 while effectively mitigating their disadvantages.

Level of prescription

40. Directive (EU) 2015/849 identifies a number of situations that firms must always treat as high risk. In some cases, Directive (EU) 2015/849 prescribes what firms must do to mitigate that risk. However, most of Directive (EU) 2015/849 contains only high-level principles and obligations.

Option 1

41. The guidelines could set out exactly what constitutes high and low risk and what firms should do in each of these situations.

42. The advantage of this approach is that a high level of prescription could reduce regulatory uncertainty and harmonise approaches across the EU. In some cases, it could also reduce the cost of compliance, as firms would not have to risk-assess individual business relationships or occasional transactions.

43. The disadvantage is that this approach is unlikely to be proportionate or effective, as firms and competent authorities will focus on compliance rather than the successful identification, assessment and management of ML/TF risk.

44. This approach also fails to take account of contextual factors that could move a business relationship or occasional transaction into a higher or lower risk category. For example, setting monetary thresholds below which a relationship should be considered low risk at European level may lead to the application of inadequate risk mitigation measures in jurisdictions where this threshold does not reflect average incomes. There is also a risk that prescribing high- and low-risk situations will lead to firms failing to identify and manage high-risk situations that are not set out in the guidelines.

45. Finally, this approach is not compatible with international AML/CFT standards and guidance.

Option 2

46. The guidelines could provide firms with information on what they need to consider when determining whether a situation presents a high or a low ML/TF risk, and which type of CDD might be appropriate to manage that risk.

47. The advantage of this approach is that it allows firms to develop a good understanding of the ML/TF risk to which they are exposed. It also enables them to focus their resources on areas of high risk, which is conducive to the adoption of proportionate and effective

AML/CFT controls.

48. The disadvantage of this approach is that it requires firms and competent authorities to have sufficient AML/CFT expertise to identify, assess and manage ML/TF risk effectively.

Preferred option

49. Option 2 is the ESAs' preferred approach, as it is conducive to the adoption, by firms, of a proportionate and effective risk-based approach.

Costs and benefits

50. The ESAs' preferred options are guidelines that:

- are consistent with relevant international standards and guidance;
- address both high and low risk factors;
- combine general guidelines for all firms with sector-specific guidelines; and
- provide firms with the tools they need to identify, assess and manage ML/TF risk in a proportionate and effective manner.

51. The ESAs expect firms and competent authorities to incur at times significant costs as they review and make changes to their approaches to comply with new national legal frameworks resulting from the transposition of Directive (EU) 2015/849 by Member States. The cost associated with the application of these guidelines will therefore be largely absorbed by the cost associated with compliance with the underlying legal change.

52. This means that these guidelines should not create significant costs for firms or competent authorities above those associated with a move to the new legal AML/CFT regime under Directive (EU) 2015/849. The benefits will follow largely from risk-sensitive guidelines, clear regulatory expectations and the harmonisation of approaches across the EU.

Firms

53. The benefits of this approach for firms are that these guidelines allow firms to adopt policies and procedures that are proportionate to the nature, scale and complexity of their activities. This means that more complex, higher risk, firms will be able to tailor their risk management to their risk profile, and firms that are exposed to low levels of ML/TF risk will be able to adjust their compliance costs accordingly.

54. All firms will face some one-off costs as a result of reviewing their internal policies and controls, making necessary adjustments to reflect these guidelines and training staff accordingly. These one-off costs will be higher for more complex firms and firms that do not already apply a risk-based approach.

55. However, these one-off costs are likely to be offset by all firms in the medium to long

term through ongoing cost reductions once the necessary adjustments have been made; furthermore, since these adjustments are likely to take place at the same time as new legislation transposing Directive (EU) 2015/849 come into effect, firms should be able to absorb the one-off costs associated with these guidelines as part of the changes they have to make to comply with their new legal and regulatory obligations. This means that the costs attributable to these guidelines will not in the end be significant.

56. In light of the considerations regarding costs and benefits set out above, the net impact of these guidelines for firms is likely to be close to zero.

Competent authorities

57. The benefits of this approach for competent authorities are that the guidelines will help supervisors set clear expectations of the factors firms should consider when identifying and assessing ML/TF risk and deciding on the appropriate level of CDD.

58. The costs to competent authorities will arise mainly from reviewing existing regulatory guidance to firms and supervisory manuals to ensure consistency with these guidelines. Competent authorities will also incur some costs from retraining staff. However, all of these costs are likely to be one-off costs that are likely to be absorbed as part of their normal work by those competent authorities that already enforce a risk-based approach. The one-off costs will be higher for competent authorities that are unfamiliar with the risk-based approach, but they are unlikely to exceed the costs arising from the implementation of national legislation transposing Directive (EU) 2015/849.

59. In light of the considerations regarding costs and benefits set out above, the net impact of these guidelines for competent authorities is expected to be close to zero, but positive.

4.2. Overview of questions for consultation

a) Do you consider that these guidelines are conducive to firms adopting risk-based, proportionate and effective AML/CFT policies and procedures in line with the requirements set out in Directive (EU) 2015/849?

b) Do you consider that these guidelines are conducive to competent authorities effectively monitoring firms' compliance with applicable AML/CFT requirements in relation to individual risk assessments and the application of both simplified and enhanced customer due diligence measures?

c) The guidelines in Title III of this consultation paper are organised by types of business. Respondents to this consultation paper are invited to express their views on whether such an approach gives sufficient clarity on the scope of application of the AMLD to the various entities subject to its requirements or whether it would be preferable to follow a legally-driven classification of the various sectors; for example, for the asset management sector, this would mean referring to entities covered by Directive 2009/65/EC and Directive 2011/61/EU and for the individual portfolio management or investment advice activities, or entities providing other investment services or activities, to entities covered by Directive 2014/65/EU.

4.3. Views of the stakeholder groups

60. The EBA's Banking Stakeholder Group (BSG) responded to this consultation.

61. The BSG considered that the draft guidelines were conducive to firms adopting risk-based AML/CFT policies and procedures. However, in some cases, greater detail was warranted to reduce the risk of national competent authorities enforcing divergent expectations of firms' assessment and management of AML/CFT risk, for example in relation to establishing a beneficial owner's source of funds, the application of CDD measures to non-face-to-face relationships and the appropriate management of lower risk correspondent banking relationships.

62. The BSG also asked for greater clarity on the relationship between these guidelines and similar international or national AML/CFT guidance.

4.4. Feedback on the public consultation

63. The ESAs publicly consulted on the draft proposal.

64. The consultation period lasted for three months and ended on 22 January 2016. Fifty-seven responses were received from representatives of or associations from the private sector, of which forty-five were published on the ESAs' websites. The EBA's Banking Stakeholder Group was among those who expressed a view.

65. This paper summarises the key points and other comments received during the public consultation, the ESAs' response and the action taken to address these comments.

66. Where several respondents made similar comments or the same respondent repeated their comments in response to different questions, these comments, and the ESAs' analysis, are included in the section of this paper where the ESAs considered them most appropriate.

67. Several changes to the draft joint guidelines have been made as a result of the responses received during the public consultation.

Summary of key issues and the ESAs' response

68. Most respondents welcomed the draft guidelines. They considered that the draft guidelines would foster a common understanding of the risk-based approach to AML/CFT and support the implementation, by firms, of an effective and proportionate risk-based approach to AML/CFT at the national level. Respondents were particularly supportive of the draft guidelines' emphasis on firms taking a holistic view of all relevant risk factors when determining the level of risk associated with a business relationship or occasional transaction, and generally found the level of detail the draft guidelines contained to be adequate.

69. Where respondents raised concerns, these broadly fell into four categories:

- the ability or preparedness of national competent authorities to apply these draft guidelines in a consistent manner;
- the status of these draft guidelines, in particular their relationship with existing national and international guidelines;
- the distinction between money laundering and terrorist financing risk factors; and
- a perceived conflict between the draft guidelines' provisions and a customer's right to a basic payment account on the one hand and the Union's data protection framework on the other.

70. The ESAs thank all respondents for taking the time to reply and for the constructive and positive feedback they received. The ESAs have carefully considered all responses and revised the guidelines where appropriate.

Ensuring the consistent application of these guidelines by national competent authorities

71. A number of respondents were concerned that these guidelines, of themselves, might not be enough to ensure the consistent supervision, by national competent authorities, of the risk-based approach to AML/CFT. Several respondents thought that the ESAs should take further action to achieve greater harmonisation of supervisory approaches across Member States and one respondent called on the ESAs to act as arbiters should firms disagree with their competent authorities' assessments.

72. These guidelines form part of the ESAs' wider work on fostering consistent supervisory practices and a common approach to AML/CFT, and need to be considered in that context. The Risk Factors Guidelines equip firms with the tools they need to make informed decisions on the effective identification, assessment and management of ML/TF risk, and set common, regulatory expectations to which national competent authorities will refer when assessing the adequacy of firms' AML/CFT systems and controls. Other ESA instruments, including the Joint Risk-Based Supervision Guidelines,[36] complement the Risk Factors Guidelines by specifying how competent authorities should organise AML/CFT supervision. Together, they provide a solid foundation for promoting a coherent and more harmonised supervisory response to AML/CFT challenges.

73. As in other areas of their work, the ESAs are providing training to competent authorities on the application of their AML/CFT standards, monitoring their implementation and keeping them under review to ensure that they remain relevant and conducive to a more robust European approach to AML/CFT. Should the ESAs become aware of competent authorities failing to apply these standards, or applying them in a way that appears to be in breach of Union law, they will take action to address this where appropriate and necessary.

The status of these draft guidelines, in particular their relationship with existing national and international guidelines

74. Several respondents sought clarity on how these guidelines sit alongside national or international AML/CFT standards such as the FATF's Recommendations and the Wolfsberg Group's AML/CFT guidance. Some thought that a number of provisions in these guidelines went beyond what international best practice suggested and called on the ESAs to reconsider their approach; consistency was important to make AML/CFT compliance easier for firms with an international footprint. One respondent wrote that they preferred national industry guidance and would be following that instead.

75. The ESAs drafted these guidelines in a way that is consistent with existing international standards and guidance. This is in line with the co-legislators' approach to Directive (EU) 2015/849, which provides a common European legal basis for the implementation of the FATF's Recommendations.

[36] Joint Guidelines on the characteristics of a risk-based approach to anti-money laundering and terrorist financing supervision, and the steps to be taken when conducting supervision on a risk-sensitive basis (2016): https://esas-joint-committee.europa.eu/Pages/Guidelines/Joint-Guidelines-on-the-Characteristics-of-a-Risk-based-Approach-to-Anti-money-Laundering-and-Terrorist-Financing-Supervisi.aspx.

76. There are, however, a number of differences between international guidance and the EU's legal framework, for example in situations where EU law creates specific obligations on firms. Regulatory guidance cannot over-ride legal provisions and, in those cases, these guidelines necessarily differ from international standards.

77. Article 16(3) of the ESAs Regulations requires competent authorities to 'make every effort to comply' with these guidelines. In practice, this means that competent authorities will incorporate these guidelines into their national framework by, for example, amending relevant legal provisions or adjusting supervisory guidance. Firms that do not adapt their approach accordingly risk being in breach of their AML/CFT obligations.

Consistency with legal provisions in Union law

78. Some respondents were concerned that compliance with these guidelines' provisions would result in a breach of a person's right to a basic payment account under Directive 2014/92/EU or the European data protection framework. One respondent in particular was concerned that expecting firms to consider a customer's reputation was against data protection rules.

79. Directive (EU) 2015/849 makes the identification and assessment of ML/TF risk and the successful application of risk-sensitive CDD controls to all customers and their beneficial owners a condition for the establishment of a business relationship. Where firms cannot comply with these obligations, they cannot enter into, or maintain, a business relationship.

80. Consequently,

- Directive 2014/92/EU provides that the right to open and use a basic payment account applies only to the extent that credit institutions can comply with their AML/CFT obligations; and

- Article 43 of Directive (EU) 2015/849 is clear that the processing of personal data for AML/CFT purposes is a matter of public interest under Directive 95/46/EC. This means that firms that collect, analyse, record or otherwise handle personal data to, for example, assess the ML/TF risk associated with a particular customer but do not use that personal data for purposes other than AML/CFT compliance, are not in breach of the Union's data protection framework.

81. These guidelines therefore comply with Union law and do not conflict with provisions in Directive 2014/92/EU or data protection rules.

Distinguishing money laundering and terrorist financing risk factors

82. A number of respondents asked for further guidance on the risks of terrorist financing, and how CFT controls are different from AML controls.

83. These guidelines do not systematically distinguish between the systems and controls firms should put in place to identify, assess and manage ML risk and those they should put in place to identify, assess and manage TF risk; guidance related to one will be relevant for the other, unless specified. This is because terrorist funds can appear legitimate and inoffensive, and, in the absence of specific intelligence from law enforcement, will be difficult to identify. The value in CFT controls therefore lies mainly in the post facto identification of terrorist networks, and, consequently, the CFT systems and controls firms will put in place, such as monitoring and other CDD measures, overlap with their AML systems and controls.

84. Attempts are now being made at the international, supranational and national levels to better understand TF risk and identify risk factors that may be conducive to a more preventative approach. These risk factors will be incorporated into these guidelines as appropriate.

Summary of responses to the consultation and the ESAs' analysis

Comments	Summary of responses received	ESAs' analysis	Amendments to the proposals
Comments on Title I			
Subject matter, scope and definitions	One respondent was concerned that the definition of 'occasional transaction' was not in line with the definition in Directive (EU) 2015/849.	Transactions can be carried out as part of a business relationship, or on a one-off, 'occasional' basis where a business relationship has not been established. As Directive (EU) 2015/849 makes clear, a business relationship 'is expected, at the time when the contact is established, to have an element of duration'. There is no expectation of an ongoing, durable relationship in the case of occasional transactions and the guidelines' definition of occasional transactions – that is, a transaction that is not carried out as part of a business relationship – is therefore in line with Directive (EU) 2015/849.	No change.
	One respondent wanted to replace 'firms' with 'obliged entities'.	'Obliged entities', for the purpose of Directive (EU) 2015/849, include some entities that are not credit or financial institutions. These guidelines apply to credit and financial institutions only.	No change.
	One respondent asked that the guidelines define 'must', 'may' and 'should'.	In line with other ESA guidelines, the Risk Factors Guidelines use 'must', 'should' and 'may' to describe different degrees of obligations on firms. 'Must' is used to describe a legal obligation, 'should' introduces a strong expectation and 'may' describes examples of possible measures firms could take to meet their legal and regulatory obligations.	Several, to identify the legal source whenever the word 'must' is used.

Comments	Summary of responses received	ESAs' analysis	Amendments to the proposals
Comments on Title II			
Assessing and managing risk – general comments	One respondent thought that firms should not be expected to do their own risk assessment. This was something national authorities should do.	Article 8 of Directive (EU) 2015/849 requires firms to identify and assess the ML/TF risk to which they are exposed.	No change.
	A number of respondents disagreed with individual risk factors, e.g. 'large transactions'. They did not believe they were indicators of higher risk.	The risk factors listed in Title II of these guidelines are not absolute and will not necessarily, of themselves, move a relationship into a higher risk category. The guidelines are clear that the overall context is important and that firms should take a holistic view of all relevant risk factors.	No change.
	One respondent considered that the guidelines' expectation that documents be kept up to date was excessive, and that firms should merely do this on a best-efforts basis	Article 13(1)(d) of Directive (EU) 2015/849 requires firms to keep documents, data or information held up to date.	No change.
	A number of respondents questioned the rationale for requiring firms to establish the nature and purpose of the business relationship, with some suggesting that this was not essential.	Establishing the nature and purpose of the business relationship is not only a requirement under Directive (EU) 2015/849, it is also central to understanding the ML/TF risk associated with the business relationship and will help firms determine what constitutes an unusual or suspicious transaction in the context of the individual business relationship. What firms do to establish the nature and purpose of the business relationship can be adjusted on a risk-sensitive basis, and Title II of these guidelines contains information on what this could entail.	No change.

Comments	Summary of responses received	ESAs' analysis	Amendments to the proposals
	Some respondents were uncomfortable with references to media searches as possible information sources and asked that these references be deleted.	The guidelines suggest a number of information sources firms can refer to when identifying the risk associated with a business relationship or occasional transaction. These include media sources, as information in the public domain can be helpful in furthering a firm's understanding of who their customers are, and in determining where further questions should be asked. The guidelines are clear that such sources should only be relied upon to the extent that they are credible and reliable. Paragraph 20 explains how firms can determine the credibility of allegations they become aware of in this way.	No change.
	Many respondents expressed strong support for the statement in paragraph 17 that firms should take a holistic view of relevant risk factors, and that isolated risk factors may not move a relationship into a higher risk or lower risk category. Some asked that this paragraph be highlighted in bold or repeated throughout the text.	This paragraph is key to the correct interpretation of these guidelines and similar statements are found throughout the text.	No change.
Customer risk factors	Several respondents commented on the beneficial ownership risk factors. They were concerned that information on beneficial owners was hard to obtain, and thought that the lesser CDD requirements in Article 13(1)(b) of Directive (EU) 2015/849 meant that fewer factors had to be considered when identifying the ML/TF risk	The guidelines do not prescribe how many risk factors firms should consider; however, firms should in any case obtain enough information on the beneficial owner to understand the risk associated with the business relationship resulting from who the beneficial owner is.	No change.

Comments	Summary of responses received	ESAs' analysis	Amendments to the proposals
	associated with the relationship because of who the beneficial owner was. One respondent was of the view that firms should not consider the ML/TF risk associated with the beneficial owner.		
	Several respondents disagreed with suggestions that firms should consider the ML/TF risk associated with a customer's or beneficial owner's business activity.	The source of funds is an important indicator of ML/TF risk.	No change.
	Some respondents argued against the guidelines' suggestion that firms consider a customer's or a customer's beneficial owner's reputation as part of their risk assessment efforts. Poor reputation was not evidence of wrongdoing and customers should always be presumed innocent unless convicted by a court.	Understanding the reputation of those involved in the business relationship is important to assess the risk that the business relationship might be used for financial crime purposes. There is no suggestion in these guidelines that allegations of wrongdoing are evidence of criminal conduct.	No change.
	Several respondents asked that the ESAs provide guidelines on the risk associated with customers who are refugees.	The EBA issued its Opinion on the application of CDD measures to customers who are asylum seekers from higher-risk third countries or territories in April 2016, which sets out how firms can apply robust AML/CFT controls while at the same time facilitating the financial inclusion of vulnerable customers.	Explanatory detail has been added to the customer risk factors section.
Countries and geographical areas	Several respondents claimed that it was unreasonable to expect firms to assess the ML/TF risk associated with a jurisdiction; some suggested that all FATF/FSRB members should instead be deemed 'equivalent', or that the ESAs should publish a list of equivalent jurisdictions.	Directive (EU) 2015/849 requires firms to identify and assess ML/TF risk. Country risk is one of the factors firms have to consider as part of this. These guidelines set out a number of risk factors firms should consider when making that assessment. FATF mutual evaluations demonstrate that	Explanatory detail has been added to facilitate the assessment of the ML/TF risk associated with

Comments	Summary of responses received	ESAs' analysis	Amendments to the proposals
		FATF/FSRB membership does not, of itself, mean that a country's AML/CFT defences are adequate.	different jurisdictions, and consequential changes have been made throughout the guidelines.
	Some respondents were concerned about references to offshore jurisdictions and tax havens. They thought these terms had unhelpful pejorative connotations and suggested that international tax cooperation was now much greater than in the past.	ML/TF risk is determined, inter alia, by a jurisdiction's commitment to international tax transparency and information sharing standards.	Explanatory detail has been added to facilitate the assessment of ML/TF risk associated with different jurisdictions, and consequential changes have been made throughout the guidelines.
Products, services and transactions risk factors	Several respondents wrote that associating non-face-to-face relationships with higher ML/TF risk conflicted with the EU's digital agenda.	Annex III to Directive (EU) 2015/849 lists non-face-to-face business relationships or transactions as potentially higher risk. In the same way, the guidelines do not suggest that non-face-to-face relationships are always high risk but instead ask firms to consider how the customer comes to the firm, which may or may not give rise to higher risk.	No change.
Weighting risk factors	Several respondents explicitly supported the statement that 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 or	This section is key to the correct interpretation of these guidelines and similar statements are found throughout the text.	No change.

Comments	Summary of responses received	ESAs' analysis	Amendments to the proposals
	occasional transaction. This was central to a proportionate, risk-based approach and should be highlighted.		
	Several respondents explicitly welcomed the guidelines on weighting, but asked that the guidelines make clear that automated systems are not warranted in all cases.	The guidelines do not prescribe the use of automated systems, but the exclusive use of manual systems should not stand in the way of effective AML/CFT systems and controls.	This section has been amended to make clear that it only applies where firms use automated systems.
Categorising business relationships	One respondent argued that only high-risk customers needed to be categorised.	The guidelines do not prescribe how firms should categorise customers, but are clear that, in line with good risk management practices, all business relationships and occasional transactions should be categorised based on the level of ML/TF risk. Correct categorisation of business relationships is key to the application of adequate CDD and risk management measures.	No change.
SDD	Several respondents argued that the guidelines did not provide for exemptions from CDD in low-risk situations; furthermore, some respondents claimed that, in low-risk situations, beneficial owners did not need to be identified.	Directive 2005/60/EC provided for exemptions from CDD obligations in low-risk situations, subject to certain conditions. It was possible, in some cases, not to identify the beneficial owner. However, Directive (EU) 2015/849 does not provide for such exemptions. This means that firms always have to apply all CDD measures in all cases, even though the extent of these measures can be adjusted on a risk-sensitive basis.	No change.
	Several respondents complained that the guidelines' SDD section was too similar to standard CDD. There was concern, in particular, about one	In line with the FATF's Recommendations, Directive (EU) 2015/849 requires firms to apply all CDD measures in all cases. As a result, SDD measures now	No change.

Comments	Summary of responses received	ESAs' analysis	Amendments to the proposals
	provision suggesting that verifying identity on the basis of a single document qualified as SDD.	closely resemble CDD measures, whereas they could have resulted in exemptions under the previous regime.	
PEPs	A number of respondents felt that the guidelines' PEPs provisions were unduly onerous. Respondents took issue with the need to establish a PEP's source of wealth and source of funds, which they considered disproportionate, and several thought that requiring senior management sign-off would lead to firms avoiding business relationships with PEPs. There were suggestions that the guidelines should establish a monetary threshold below which PEP relationships were not high risk, and that the ESAs should publish PEP lists. Some respondents took issue with the guidelines' suggestion that PEP relationships did not always present the same degree of high risk, while others explicitly welcomed this as sensible and proportionate.	Article 20 of Directive (EU) 2015/849 requires firms to apply specific EDD measures to business relationships or transactions with PEPs. These EDD measures have to be applied in all cases and include the establishment of the PEP's source of wealth and source of funds, and the need for senior management approval for establishing or continuing a business relationship with a PEP. There is no exemption, in the Directive, for business relationships with PEPs that remain below a certain threshold. The Directive does, however, permit the adjustment of the extent of obligatory EDD measures on a risk-sensitive basis and the guidelines set out how this can be done.	No change.
High-risk jurisdictions and other high-risk situations	Most respondents agreed with this section but some respondents argued that information on a customer's family members or business associates should not influence the risk assessment. Others asked that the EDD measures in this section be ranked according to their importance.	In higher risk situations, information about a customer's family or close business partners can provide firms with important insights into the ML/TF risk associated with the business relationship, for example where allegations of corruption or other serious crimes exist that could increase the risk of the firm handling the proceeds of crime. It is not possible to rank EDD measures by	No change.

Comments	Summary of responses received	ESAs' analysis	Amendments to the proposals
		importance as the relevance or relative importance of each measure will depend on the reason why a relationship is classed as higher risk.	
Other considerations	One respondent suggested that guidelines asking firms to terminate a business relationship where they are not satisfied that the purpose and nature of the business relationship are legitimate were not in line with Directive (EU) 2015/849. Others explicitly welcomed this provision.	The guidelines are clear that firms should enter into business relationships only where they are satisfied that they can manage the ML/TF risk. Where firms have reasonable grounds to suspect ML/TF, they must report their suspicion to the FIU.	No change.
Derisking	Several respondents welcomed guidance on derisking, although some asked that the guidelines make clear that the risk-based approach, of itself, does not require the termination of higher risk relationships and provided drafting suggestions.	This clarification is in line with the FATF's derisking statements.	This paragraph has been amended in line with respondents' drafting suggestions.
Comments on Title III			
Correspondent banking	Some respondents considered that EDD measures should not apply to correspondent relationships where banks acted in a principal-to-principal capacity.	The guidelines acknowledge that not all correspondent relationships present the same level of risk and provide guidance to firms on how to adjust their EDD measures accordingly; however, the definition of correspondent relationships in Directive (EU) 2015/849 is broad and it is not possible for these guidelines to exclude specific correspondent relationships, even if firms consider these to be associated with lower levels of ML/TF risk.	Minor amendments to better reflect different levels of high risk in line with international guidance.

Comments	Summary of responses received	ESAs' analysis	Amendments to the proposals
	Several respondents argued that reliance on the Wolfsberg questionnaire should, of itself, be enough to meet the Directive's correspondent banking requirements.	Questionnaires are a good starting point but may not be enough to allow firms to comply with their obligations under Directive (EU) 2015/849 as transposed by Member States.	Minor amendments to clarify regulatory expectations.
Retail banking	Several respondents pointed to a perceived incompatibility between this chapter's reference to non-resident customers as potential indicators of higher risk and Directive 2014/92/EU.	Directive 2014/92/EU does not prevent the assessment of the ML/TF risk associated with a business relationship or occasional transaction and is clear that the right to open and use a basic payment account applies only to the extent that credit institutions can comply with their AML/CFT obligations.	No change.
	A clarification was requested on which CDD obligations could be met in lower risk situations by referring to a payment drawn on an account in the customer's name in an EEA country.	In lower risk situations, a payment drawn on an account in the customer's name in an EEA country may be enough to satisfy the requirements of Article 13(1)(a) and (b).	Minor amendments to clarify regulatory expectations.
	Most respondents welcomed the provisions on pooled accounts, but several asked that they be extended to apply to equivalent jurisdictions as well.	The guidelines have been amended to allow the application of SDD measures in situations where the account holder is a firm in a non-EEA jurisdiction, provided that this jurisdiction's AML/CFT regime is not less robust than the regime envisaged in Directive (EU) 2015/849 and that the firm is supervised effectively for compliance with these obligations. This provision has not been extended to other obliged entities in third countries on account of the ML/TF risk associated with obliged entities that are	Extended to equivalent countries, but only for 'firms'.

Comments	Summary of responses received	ESAs' analysis	Amendments to the proposals
		not firms as defined in these guidelines.	
E-money issuers	Several respondents suggested that low thresholds alone were sufficient to put an e-money product into a lower risk category.	The guidelines describe low thresholds as a factor indicating lower risk but are clear that a low threshold may not be enough to reduce terrorist financing risk. Firms have to take a holistic view of all the relevant risk factors, which, together, determine the level of ML/TF risk associated with a business relationship.	Minor changes to clarify regulatory expectations.
	One respondent was concerned that scheme-enabled cards were described as higher risk.	The ability to use an e-money product widely can give rise to higher ML/TF risk, but the guidelines are clear that firms have to take a holistic view of all the relevant risk factors that, together, determine the level of ML/TF risk associated with a business relationship.	No change.
	One respondent suggested that distributors will be unable to spot unusual multiple purchases or e-money product usage. They said that such behaviour was visible to issuers only.	There is no expectation that distributors will monitor customer behaviour after e-money has been issued. However, where a distributor who is themselves an obliged entity observes unusual behaviour at point of sale, this could indicate higher risk.	Minor changes to clarify regulatory expectations.
	One respondent asked for examples of adequate safeguards that might reduce the risk associated with non-face-to-face relationships.	Examples of adequate safeguards include electronic identification in line with Regulation (EU) No 910/2014 and anti-impersonation fraud checks.	Minor changes to clarify regulatory expectations.
	One respondent thought that issuers could not check whether a payment had been drawn on an account in the sole or joint name of the customer, and suggested that issuers should look to establish whether the customer could be shown to have	Establishing control over an account without establishing who the holder is does not meet the CDD requirements set out in Article 13(1) of Directive (EU) 2015/849.	No change.

Comments	Summary of responses received	ESAs' analysis	Amendments to the proposals
	control over the account instead.		
	Several respondents considered that restricting the ability to reduce the intensity of ongoing monitoring to e-money products that do not exceed EUR 250 over a 12-month period was not risk-based.	Ongoing monitoring is important to understand ML/TF risk and any reduction in the intensity of ongoing monitoring has to be considered in that context. However, firms will be able to ascertain at what point transaction volumes and values cease to be low risk.	The monetary threshold has been removed.
Money remitters	A number of respondents disagreed with some higher risk indicators. These were not, of themselves, suggestive of higher ML/TF risk. Others suggested additional risk factors.	The guidelines are clear that firms should take a holistic view of relevant risk factors, and that isolated risk factors may not move a relationship into a higher risk or lower risk category.	Minor changes to clarify regulatory expectations.
	One respondent was unclear about whether the guidelines sanctioned the establishment of a business relationship or occasional transactions where CDD information was missing.	Directive (EU) 2015/849 and Regulation (EU) 2015/847 set out which information on the payer or the payee must always be obtained and verified. The guidelines recognise that many money remitters' business is primarily transaction based, and no business relationships are established. This limits what the money remitter knows about the payer or the payee, which is why this chapter sets out what a money remitter's systems should be capable of to ensure ML/TF is detected.	Minor changes to clarify regulatory expectations.
Wealth management	Several respondents suggested that it was unreasonable for wealth managers to visit the clients' location in high-risk cases.	The guidelines provide examples of EDD measures wealth managers could take in high-risk situations, but do not prescribe EDD measures. Title II of these guidelines is clear that what is appropriate will depend on the reason why a relationship was classified as high risk.	No change.

Comments	Summary of responses received	ESAs' analysis	Amendments to the proposals
	Several respondents objected to the guidelines' suggestion that SDD was not appropriate in a wealth management context.	The application of SDD measures is reserved for low-risk situations. Annex III to Directive (EU) 2015/849 describes private banking as potentially higher risk, as the nature of wealth management, and many of the features typically associated with wealth management, are indicative of higher ML risk. This means that SDD measures are not appropriate in this context.	No change.
Life insurance	A number of respondents disagreed with various risk factors.	The guidelines are clear that firms should take a holistic view of relevant risk factors, and that isolated risk factors may not move a relationship into a higher risk or lower risk category.	No change.
Investment funds	A number of respondents asked for clarification on which party is responsible for the application of CDD measures.	The responsibility for applying CDD measures remains with the fund or the fund manager.	The guidelines have been redrafted to clarify CDD requirements in the funds distribution context.
	Several respondents considered that it was unreasonable to require investment funds to identify investors where intermediaries were used.	Directive (EU) 2015/847 is clear that firms have to identify, and verify the identity of, the customer and the beneficial owner. Beneficial owners are natural persons who own or control the customer, or on whose behalf a transaction is being conducted. The guidelines set out how funds and fund managers can meet their CDD requirements in low-risk situations.	The guidelines have been redrafted to clarify CDD requirements in the funds distribution context.