JOINT COMMITTEE OF THE EUROPEAN SUPERVISORY AUTHORITIES

21 October 2015
JC 2015 061

Joint Consultation Paper

Joint Guidelines under Article 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. Responding to this Consultation

The European Supervisory Authorities (the ESAs) invite comments on all proposals put forward in this paper and in particular on the specific questions summarised in 5.2.

Comments are most helpful if they:

- respond to the question stated;
- indicate the specific point to which a comment relates;
- contain a clear rationale;
- provide evidence to support the views expressed/ rationale proposed; and
- describe any alternative regulatory choices the ESAs should consider.

Submission of responses

To submit your comments, click on the 'send your comments' button on the consultation page by 22 January 2016. Please note that comments submitted after this deadline, or submitted via other means may not be processed.

Publication of responses

Please clearly indicate in the consultation form if you wish your comments to be disclosed or to be treated as confidential. A confidential response may be requested from us in accordance with the ESAs' rules on public access to documents. We may consult you if we receive such a request. Any decision we make not to disclose the response is reviewable by the ESAs' Board of Appeal and the European Ombudsman.

Data protection

The protection of individuals with regard to the processing of personal data by the ESAs is based on Regulation (EC) N° 45/2001 of the European Parliament and of the Council of 18 December 2000 as implemented by the ESAs in their implementing rules adopted by their Management Boards. Further information on data protection can be found under the Legal notice section of the ESAs' website.

2. 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 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 Europe's anti-money laundering (AML) and counter-terrorist financing (CFT) regime. It recognises that the risk of money laundering and terrorist financing 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.

Article 17 and 18(4) of Directive (EU) 2015/849 require the European Supervisory Authorities 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 money laundering and terrorist financing risk associated with a business relationship or occasional transaction. They also set out how firms can adjust the extent of their customer due diligence measures in a way that is commensurate to the money laundering and terrorist financing 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 generic 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 money laundering and terrorist financing risk associated with individual business relationships or occasional transactions.

- Title III is sector specific and complements the generic 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 Customer Due Diligence measures by firms in those sectors.

These guidelines will help firms identify, assess and manage the money-laundering and terrorist financing 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.

Next steps

These guidelines are likely to be finalised in Spring 2016.

Once adopted, the ESAs will keep these guidelines under review and update them as appropriate.

3. 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 Financial Action Task Force (FATF), an international anti-money laundering and counter-terrorist financing 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 anti-money laundering (AML) and counter-terrorist financing (CFT) regime. It recognises that the risk of money laundering and terrorist financing 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, Customer Due Diligence (CDD) is central to this process, both for 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 his 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.

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

The Directive therefore requires the European Supervisory Authorities 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 where simplified due diligence or enhanced due diligence 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 money-laundering and terrorist financing 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 money laundering or terrorist financing risk associated with individual business relationships or occasional transactions.

Countering the financing of terrorism

Many of the controls firms have in place in relation to counter the financing of terrorism will overlap with their AML measures. These may cover, for example, risk assessment, customer due diligence 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.

4. Joint Guidelines under Article 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 subparagraph 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 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 respective ESA whether they comply or intend to comply with these Joint Guidelines, or otherwise with reasons for non-compliance, by dd.mm.yyyy (two months after issuance). In the absence of any notification by this deadline, competent authorities will be considered by the respective 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/201x/xx'. 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 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 for 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 European Supervisory Authorities have issued guidelines on risk-based supervision in accordance with Article 48(10) of Directive (EU) 2015/849.

7. Compliance with the European 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 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.

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

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

9. These Guidelines come in two parts. Title II is generic 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 a business relationship or 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 effect, 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 (CDD).

  Firms should use the findings from their business-wide risk assessment to decide 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 Articles 13 (1) (a), (b) and (c) and Article 14(4) of Directive (EU) 2015/849. Initial CDD should at least include 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 source and, where applicable, verify the beneficial owner's identity in 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.

- Monitoring and Review.

  Firms must keep their risk assessment up to date and under review. Firms must monitor transactions to ensure that these are in line with the customer's risk profile and business and, where necessary, examine the source of funds, to detect possible money laundering or terrorist financing. 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.

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 geographic areas they operate in, 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. Firms should determine the type and numbers of sources on a risk-sensitive basis.

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 black lists;
- information from media sources, such as newspaper reports;
- information from 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 should consider all risk factors in all cases. Firms should take a holistic view of the risk associated with the situation and note that unless required by Directive (EU) 2015/849 or national legislation, 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[3], firms should consider the risk related to:

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

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

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

c) the customer's and the customer's beneficial owners' nature and behaviour.

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

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

- Does the customer or beneficial owner have links to sectors that are associated with higher ML or 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, what is the purpose of their establishment?

- 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 enhanced due diligence measures in line with Article 20 of Directive (EU) 2015/849.

- Does the customer or beneficial owner hold another public position that might enable them to abuse public office for private gain?

- Is the customer a legal person subject to enforceable disclosure requirements that ensure that reliable information about the customer's beneficial owner is publicly available, for example public companies listed on stock exchanges that make such disclosure a condition for listing?

- Is the customer a credit or financial institution from a jurisdiction with an effective AML/CFT regime and is it supervised for compliance with local AML/CFT obligations?

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

- Is the customer's or their beneficial owner's background consistent with what the firm knows about their former, current or planned business activity, their business' 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 their beneficial owners' reputation:

- Are there any adverse media reports about the customer, for example are there any allegations of criminality or terrorism (proven or not) against the customer or their beneficial owners? If so, are these credible? Firms should determine the credibility of allegations on the basis of the quality and independence of the source data and the persistence of reporting of these allegations, among others.

- Is the customer, beneficial owner or anyone associated with them subject to an asset freeze due to 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 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 subject to a suspicious activity report in the past?

- Are there suggestions that the customer or beneficial owner or anyone associated with them may have handled the proceeds from crime?

- Does the firm have any in-house information about the customer's or their 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 their beneficial owners' nature and behaviour:

- 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?

- 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 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 apparent economic or lawful purpose or a sound commercial rationale? Are there grounds to suspect that the customer is trying to evade certain thresholds?

- 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 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?

- Does the customer use their products and services 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 or lawful rationale for the customer requesting the type of financial service sought?

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

Countries and geographic areas

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

    a) the jurisdiction in which the customer or beneficial owner is based;

    b) the jurisdictions which are the customer´s or beneficial owner's main place of business; and

    c) the jurisdiction to which the customer or beneficial owner has relevant personal links.

23. Risk factors firms should consider when identifying the level of ML/TF risk associated with a jurisdiction include:

    - Is the country a Member of the Financial Action Task Force (FATF) or a FATF-style regional body, *e.g.* MoneyVal, that assess their members for compliance with the FATF's Recommendations and publishes their assessment?

    - Is there information from more than one credible and trustworthy 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 FATF Mutual Evaluations, the FATF's list of high risk and non-cooperative jurisdictions, International Monetary Fund assessments, Financial Sector Assessment Programme reports (FSAPs) and Organisation for Economic Co-operation and Development (OECD) reports.

    - Is there information, for example from law enforcement or the media, suggesting that a jurisdiction provides funding or support for terrorist activities or that designated terrorist organisations are operating in the country?

- 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 and the European Union ?

- Is the jurisdiction a known tax haven, secrecy haven or offshore jurisdiction?

- Is there information from credible sources about the level of predicate offences to money laundering, for example corruption, organized crime or fraud? Examples include Transparency International's Corruption Perceptions Index; OECD country reports on the implementation of the OECD's anti-bribery convention; and the UNODC World Drug Report.

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

- Is the jurisdiction politically stable?

- Is there information from more than one credible and trustworthy source about the level of international cooperation and information exchange with foreign public authorities? Examples of credible sources include FATF Mutual Evaluations and reports from the Global Forum on Transparency and Exchange of Information for Tax Purposes.

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

24. Where firms deal with natural or legal persons established in third countries that the Commission has identified as presenting a high money laundering risk, firms must always apply enhanced due diligence measures.[4]

Products, services and transactions risk factors

25. 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 afford;

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

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

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

26. 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 facilitate or allow anonymity or opaqueness of customer, ownership or beneficiary structures, for example certain pooled accounts, bearer shares, fiduciary deposits, offshore and certain onshore trusts and dealings with shell companies?

- To what extent is it possible for a third party that is not part of the business relationship to give instructions, *e.g.* certain correspondent banking relationships?

27. 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 involves multiple parties or multiple jurisdictions, for example certain trade finance transactions? Are transactions straightforward, for example regular payments into a pension fund?

- To what extent do products or services allow payments from third parties or accept overpayments where this is not normally foreseen, *e.g.* certain mortgage, pension or life insurance products? Where third party payments are foreseen, does the firm know the third party's identity, for example 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?

28. 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, such as 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 of levels of premium that could limit the use of the product or service for money laundering or terrorist financing purposes?

Delivery channel risk factors

29. When identifying the risk associated with the way 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 to the firm.

30. When assessing the risk associated with the way the customer obtains the product 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 from other parts 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 EEA standards in line with Article 28 of Directive (EU) 2015/849, for example has it considered the findings of relevant internal audit reports?

- Has the customer been introduced from a third party, for example an independent agent and is the third party a financial institution or is their 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, among others 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, *i.e.* 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, are they:

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

  ii. 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 because the intermediary has been

sanctioned for breaches of AML/CFT obligations?

iii. based in a high-risk jurisdiction?

Assessing ML/TF risk

31. Firms should take a holistic view of the ML/TF risk factors they have identified that, together, will determine the level of money laundering and terrorist financing risk associated with a business relationship or occasional transaction.

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

Weighting risk factors

33. 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 high risk jurisdiction is less relevant in light of the features of the product they seek.

34. 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 business relationships to be classified as high risk;
- situations identified by Directive (EU) 2015/849 or national legislation as always presenting a high money laundering risk cannot be over-ruled by the firm's weighting; and
- they are able to override automatically generated risk scores where necessary. The rationale for the decision to override such scores should be documented appropriately.

35. Where a firm does not develop automated systems to allocate overall risk scores to categorise business relationships or occasional transactions 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. Firm must always be able to satisfy itself that the scores allocated reflect the firm's understanding of ML/TF risk and it should be able to demonstrate this to the competent authority.

Categorising business relationships and occasional transactions

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

37. 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

38. 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.

39. As part of this, firms must apply each of the CDD measures, 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.

40. 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 money laundering and terrorist financing risks.

Simplified Customer Due Diligence

41. To the extent permitted by national legislation, firms may apply simplified customer due diligence (SDD) measures in situations where the ML/TF risk associated with a business relationship is 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 identified.

42. Simplified customer due diligence 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, such as:

  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, i.e. firms must ensure that the customer or beneficial owner's identity will ultimately be verified;

b) the threshold or time limit is set at a reasonably low level;

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 the AML Regulation or provisions in national legislation, does not permit this.

- adjusting the quantity of information obtained for identification, verification or monitoring purposes, such as:

  i. verifying identity on the basis of one document 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:

  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;

  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, *e.g.* 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 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.

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

44. The information a firm obtains when applying SDD measures must enable the firm to be reasonably satisfied that the risk associated with the relationship is low. 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.

45. Where there are indications that the risk may not be low, for example where there are grounds to suspect that money laundering or terrorist financing is being attempted or where the firm has doubts about the veracity of the information obtained, SDD must not be applied. Equally, where specific high-risk scenarios apply and there is an obligation to conduct enhanced due diligence, simplified due diligence must not be applied.

Enhanced Customer Due Diligence

46. Firms must apply enhanced customer due diligence (EDD) measures in higher risk situations to manage and mitigate those risks appropriately[5]. EDD measures do not substitute regular CDD measures but must be applied in addition to regular CDD measures.

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

    i. where their customer, or their customer's beneficial owner, is a PEP[6];

    ii. where a firm enters into a correspondent relationship with a respondent institution from a non-EEA state[7];

    iii. where a firm deals with natural persons or legal entities established in high risk third countries,[8] and

    iv. all complex and unusually large transactions, or unusual patterns of transactions, that have no obvious economic or lawful purpose.[9]

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

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

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

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

[5] Article 18-24 of Directive (EU) 2015/849.
[6] Articles 20-24 of Directive (EU) 2015/849.
[7] Article 19 of Directive (EU) 2015/849.
[8] Article 18(1) of Directive (EU) 2015/849.
[9] Article 18(2) of Directive (EU) 2015/849.

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

Politically Exposed Persons

49. 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 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.

50. 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.

Correspondent relationships

51. Firms must take specific EDD measures where they have a cross-border correspondent relationship with a respondent who is based in a third country.[10] Firms must apply all of these measures and should adjust the extent of these measures on a risk-sensitive basis.

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

52. 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

53. 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 to the customer's normal activity or the pattern of transactions associated with similar customers, products or services; or
- they are very complex compared to other, similar transactions by 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 has to apply EDD measures.

54. 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 jurisdictions and other high risk situations

55. When dealing with natural persons or legal persons established or residing in a high risk third country identified by the Commission[11] and in all other high risk situations, firms should take an informed decision which EDD measures are appropriate for each high risk situation. The appropriate type of EDD, including the extent of additional information sought, and of the increased monitoring carried out, will depend on the reason why a relationship was classified as high risk.

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

56. Firms will not need to apply all 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.

57. EDD measures firms should apply may include:

- increasing the quantity of information obtained for CDD purposes:

  i. 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 known. 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. 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. It includes obtaining information on:

     a. the number, size and frequency of transactions that are likely to pass through the account to be able to spot deviations that may give rise to suspicions. In some cases, requesting evidence may be appropriate;

     b. why the customer looks 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; or

     d. the nature of the customer's or beneficial owner's business 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 in the customer´s name with a bank subject to similar CDD standards; or

  ii. establishing that the customer's source of wealth and source of funds that are used in the business relationship are not the proceeds from criminal activity and that they 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 increased, verifying the source of wealth and the source of funds may be the only adequate risk mitigation tool. The sources of funds or wealth can be verified, among others, 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 it no longer corresponds to its 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 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 may give rise to suspicion of money laundering or terrorist financing. This may include establishing the destination of funds or ascertaining the reason for certain transactions.

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

Other considerations

59. Firms should not enter into a business relationship they are unable to comply with their CDD requirements, where they are not satisfied that the purpose and nature of the business relationship are legitimate or where they are not satisfied that they can effectively manage the risk that they may be used for money laundering and terrorist financing 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.

60. Firms should note that the application of a risk-based approach does not 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 relationship will vary, even within one category.

61. Where firms have reasonable grounds to suspect that money laundering or terrorist

financing is being attempted, firms must report this to their FIU.

Monitoring and Review

62. Firms should keep their assessment of ML/TF risk associated with individual business relationships and occasional transactions as well as 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 the business relationship and consider whether this affects the risk assessment.

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

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

- processes to ensure internal information is reviewed regularly to identify trends and emerging issues, both in relation to individual business relationships and the firm's business;
- processes to ensure the firm regularly reviews relevant information sources such as those set out 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 the firm is active in;
  ii. regularly reviewing law enforcement alerts and reports; and
  iii. regularly reviewing thematic reviews and similar publications issued by competent authorities.
- processes to capture and reviewing information on risks relating to new products;
- engagement with other industry representatives and competent authorities (such as round tables, conferences and training) and processes to feed back any findings to relevant staff; and
- establishing a culture of information sharing within the firm and strong company ethics.

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

- setting a date at which the next risk assessment update takes place, *e.g.* on the 1 March every year, to ensure new or emerging risks are included in the risk

assessment. Where the firm is aware that a new risk has emerged, or an existing one has increased, this should be reflected in the risk assessment as soon as possible; and

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

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

Record keeping

67. Firms should record and document their risk assessment of the business relationship as well as any changes brought to the risk assessment as part of their reviews and monitoring to be able to demonstrate to their competent authorities that their risk assessment and associated risk management measures are adequate.

Title III - Sector-specific guidelines

68. The sector-specific guidelines in Title III complement the generic part in Title II of these guidelines. They should be read in conjunction with Title II of these guidelines.

69. 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.

70. 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.

71. Each chapter in Title III also sets out examples of the CDD measures firms should apply on a risk-sensitive basis in either high or, 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

72. 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.

73. In a correspondent banking relationship, the correspondent processes transactions for the respondent's customers. 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 is included in the payment instruction.

74. 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

75. The following factors may indicate higher 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 correspondent banking).

- 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.

76. The following factors may indicate lower risk:

- The relationship is limited to a SWIFT RMA plus capability, which is designed to manage communications between financial institutions. This means that the respondent, or counterparty, does not have a payment account relationship. Banks are acting in a principal-to-principal capacity, rather than process transactions on behalf of their underlying clients, e.g. 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 such a transaction does not involve a payment to a third party.

Customer risk factors

77. The following factors may indicate higher 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, their 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 they are based in;
- the respondent's management or ownership includes PEPs, in particular where these are from high risk jurisdictions, or their reputation or level of expertise gives rise to concern;
- 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 their knowledge of the nature and size of the respondent.

78. The following factors may indicate lower risk, provided that the correspondent is satisfied that:

- the respondent's AML/CFT controls are in line with those required by Directive (EU) 2015/849;
- the respondent is subject to effective AML supervision;
- the respondent is part of the same group as the correspondent and the respondent complies with group AML standards that are in line with those required by Directive (EU) 2015/849.

Country or geographic risk factors

79. The following factors may indicate higher risk:

- the respondent is based in a high-risk jurisdiction;[12]

[12] See also Title II.

- the respondent conducts significant business with a high risk jurisdiction;
- the respondent's parent is headquartered or has their seat in a high-risk jurisdiction.

80. The following factors may indicate lower risk:
    - the respondent is based in an EEA Member State;
    - the respondent is based in a third country, which has AML/CFT requirements that are consistent with the 2012 FATF Recommendations and effectively implements those requirements.

Measures

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

82. Article 19 of Directive (EU) 2015/849 does not apply to cross-border correspondent relationships with respondent institutions from EEA countries, but the correspondent must still carry out CDD on the respondent, who is the correspondent´s customer, on a risk-sensitive basis.

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

84. 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. They are therefore unlikely, by themselves, to help correspondents comply with their CDD obligations.

Respondents based in non-EEA countries

85. 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.

[13] See below under "III. Measures".

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

87. Correspondents should always adequately document their EDD measures and decision-making process.

88. 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 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 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 their 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/CTF controls. This implies that the correspondent should carry out a qualitative assessment of the respondent's AML/CTF control framework, not just obtaining a copy the respondent's AML policies and procedures. This assessment should be documented appropriately. In higher risk cases, and in particular where the volume of correspondent banking transactions is substantive, the correspondent should consider on-site visits 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 respective 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.* by

other banks through their relationship with the respondent). Where the risk associated with the relationship is increased, it may be appropriate for the correspondent to satisfy themselves that the respondent complies with their responsibilities under this agreement, for example through ex-post transaction monitoring.

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

89. Pursuant to Article 13 of Directive (EU) 2015/849, correspondents should monitor these correspondent relationships to detect 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 correspondent banks allow the respondent's customers direct access to accounts (*e.g.* payable-through accounts), they should conduct enhanced ongoing monitoring of the business relationship.

Respondents based in EEA countries

90. 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. This means that correspondents must:

- identify, and verify the identity of, the respondent and their beneficial owners. As part of this, correspondents should obtain sufficient information about the respondent's business and reputation to establish that the money-laundering risk 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 they attract, and about the quality of their AML systems and controls (including publically 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.

- 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 how and by whom the

correspondent banking facility can be used (e.g. 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. Due to the nature of correspondent banking, post-execution monitoring is the norm; and

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

91. Correspondents must also establish that the respondent does not permit its accounts to be used by a shell bank[14] in line with Article 24 of Directive (EU) 2015/849. This may include asking the respondent for confirmation that they do not deal with shell banks, having sight of relevant passages in the respondents' policies and procedures or considering publicly available information, such as legal provisions that prohibit the servicing of shell banks.

92. 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.

93. Conversely, where the respondent is based in an EEA country and the risk associated with that correspondent relationship is low, SDD may be appropriate, provided that:

- the relationship is subject to adequate transaction monitoring, and

- the application of such measures is permitted by national legislation.

94. Where correspondents consider applying SDD measures, they should follow the guidelines in Title II.

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

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 money laundering and terrorist financing risk associated with individual relationships and spotting suspicious transactions more 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 indicate higher risk:

- the product's features might favour anonymity;
- the product allows payments from unidentified or un-associated third parties 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 in particular where these are not yet well understood;
- an unusually high volume or large value of transactions.

99. The following factors may indicate lower risk:

- The product has limited functionality, for example

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

ii. a product where the benefits cannot be realised for the benefit of third persons or are only realisable in the long term;

iii. a low value loan facility where the legal and beneficial title to the asset is not transferred to the customer until the contractual relationship is terminated;

- The product can only be held by certain categories of customers, *e.g.* pensioners, parents on behalf of their children, minors until they reach the age of majority, refugees or asylum seekers;

- Transactions must be carried out through an account in the customer's name at a credit or financial institution that is subject to AML/CTF requirements equivalent to those required by Directive (EU) 2015/849;

- There is no overpayment facility.

Customer risk factors

100. The following factors may indicate higher 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 extractive industries or arms trade;

  iv. the customer is a non-profit organisation that supports jurisdictions associated with an increased terrorist financing risk;

  v. the customer is a new undertaking without adequate business profile or track record;

  vi. the customer is a non-resident;

  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 behaviour or transaction volume is not in line with that expected from the category of customer to which he belongs, or is not expected based on the information the customer provided at account opening;

iii. the customer's behaviour is unusual, for example the customer unexpectedly and without reasonable explanation accelerates an agreed repayment schedule, either by means of lump sum repayments, or early termination; deposits or demands pay-out 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 factors may indicate lower 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;
- The customer is a public company listed on a regulated market and is subject to disclosure requirements that ensure adequate transparency of beneficial ownership;
- The customer is a domestic public administration or enterprise or a public administration or enterprise from a jurisdiction with low levels of corruption;
- The customer is a credit or financial institution from a jurisdiction with an effective AML/CFT regime and is supervised for compliance with their AML/CFT obligations.

Country or geographic risk factors

102. The following factors may indicate higher risk:

- The customer has significant personal or business links to high risk countries, including those identified by the Commission as having strategic AML/CFT deficiencies and jurisdictions with higher levels of predicate offences such as those related to the narcotics trade, smuggling, corruption and counterfeiting.

103. The following factors may indicate lower risk:

- Countries associated with the transaction have an AML/CTF regime comparable to 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 indicate higher risk:

- non-face to face business relationships, where no additional safeguards 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.

Measures

105. 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 systems should never be considered as a substitute for staff vigilance.

Enhanced customer due diligence

106. Where the risk associated with a business relationship or occasional transaction is increased, banks must apply EDD measures which 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 that 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;
- 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 sought include:
    i. establishing the nature of the customer's business or employment;
    ii. establishing the source of the customer's funds to ascertain that this is legitimate;
    iii. establishing the destination of the customer's funds;
    iv. understanding any associations the customer might have with other jurisdictions (headquarters, operating facilities, branches etc) and the individuals who may influence its operations;

v. where the customer is based in another country, establishing 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 increased, banks should review the business relationship annually.

Simplified customer due diligence

107. 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 the identity based on evidence of the customer being subject to that regime, for example 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 name at a regulated credit or financial institution in an EEA country satisfies the requirements stipulated by Articles 13(1) and (2) of Directive (EU) 2015/849;

- accepting alternative forms of identity, such as a letter from a government agency or other reliable public body in the customer's name, where there are reasonable grounds why the customer is unable 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.

SDD and pooled accounts

108. To the extent permitted by national legislation, where a bank's customer opens a 'pooled account' in order to administer funds that belong to their own clients, the bank may apply SDD measures provided that:

- the customer is subject to AML/CFT obligations in an EEA state and is supervised 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 others; and

- the bank is satisfied that the customer applies robust and risk-sensitive CDD measures to their own clients and their 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 or by sample-testing the customer's ability to provide CDD information upon request.

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

- identifying and verifying the identity of customer, including the customer's beneficial owners;

- assessing the purpose and intended nature of the business relationship;

- conducting ongoing monitoring of the business relationship; and

- establishing that the customer will provide upon request relevant information on their underlying clients, who are the beneficial owners of funds held in the pooled account.

110. Where the customer is established in a third country or where there are indications that the risk associated with the business relationship may not be low, firms providing retail banking services shall apply CDD measures or EDD measures as appropriate . Where the customer is established in a third country that has been identified as high risk under Article 9 of Directive (EU) 2015/849, firms providing retail banking services shall apply EDD measures.

Chapter 3: Sectoral guidelines for electronic money issuers

111. This chapter provides guidelines for electronic money issuers (E-money issuers) as defined in Article 2(3) of Directive 2009/110/EC. The degree of ML/TF risk associated with electronic money[15] (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.[16]

112. 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

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

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

114. The following factors may indicate higher risk:

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

[15] Article 2(2) of Directive 2009/110/EC.
[16] Article 3(4) of Directive 2009/110/EC.

i. can be 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. can be funded with payments from unidentified third parties.

- 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 increased financial crime risk, *e.g.* 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;

vi. allows cash withdrawals.

115. The following factors may indicate lower risk:

- Thresholds: the product

i. sets low value limits on payments, loading or redemption, including cash withdrawal;

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

iii. limits the amount of funds to 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 drawn from an account held in the customer´s name at an EEA credit or financial institution;

- Utility and negotiability: the product

i. does not allow or strictly limits cash withdrawal;

ii. can only be used domestically;

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

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

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

Customer risk factors

116. The following factors may indicate higher risk:

- the customer purchases several E-money products from the same issuer or frequently reloads the product, or make several cash withdrawals, in a short period of time and without economic reasons; where distributors are obliged entities themselves, this also applies to E-money products from different issuers;
- the customer's transactions always stay 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);
- frequent changes in customer´s identification data, such as home address, IP-address, linked bank accounts;
- the product is not used for the purpose it was designed for, *e.g.* it is used overseas when it was designed as a shopping centre gift card.

117. The following factor may indicate lower risk:

- The product is available only to certain categories of customers, *e.g.* social benefit recipients.

Distribution channel risk factors

118. The following factors may indicate higher risk:

- online and non-face to face distribution without adequate safeguards;
- distribution through intermediaries that are not themselves obliged entities under Directive (EU) 2015/849, 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 themselves that the intermediary has in place adequate AML/CFT systems and controls.

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

Country or geographic risk factors

119. The following factors may indicate higher risk:

- The payee is located in a high risk jurisdiction;[17]
- The product receives funds from sources in a high risk jurisdiction.

Measures

120. National legislation may provide for an exemption from identification and verification of the customer's and beneficial owners' identities and the assessment of the nature and purpose of the business relationship for certain E-money products according to Article 12 of Directive (EU) 2015/849, subject to the following conditions:

- A non-reloadable E-money product must:
  i. have a storage limit that does not exceed:
     a. EUR 250 where the product can be used in other jurisdictions; or
     b. EUR 500 where the product can only be used domestically, provided that national legislation allows this.
  ii. not permit more than EUR 100 to be redeemed or withdrawn in cash;
  iii. not be funded with anonymous E-money; and
  iv. be used to purchase goods and services only.
- A reloadable E-money product must:
  i. have a storage limit that does not exceed EUR 250 or EUR 500 provided that domestic legislation allows this);
  ii. be usable only in the Member State where it was issued;
  iii. have a monthly transaction limit that does not exceed EUR 250;
  iv. not permit more than EUR 100 to be redeemed or withdrawn in cash;

[17] See Title II

v. not be funded with anonymous E-money; and

vi. be used to purchase goods and services only.

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.

121. 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 it was not designed for; the firm may be able to disable the product either manually or through on-chip controls until they have been able to satisfy themselves 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 to data held on other business relationships, and that can identify patterns such as the same funding instrument or same contact details;

- systems that identify whether the product is used with merchants dealing in goods and services that are associated with increased financial crime risk.

Enhanced customer due diligence

122. 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 (such as 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 the customer about their business or jurisdictions they intend to transfer E-money to;

- obtaining information about the merchant/payee, in particular where the E-money issuer has grounds to suspect that their products are being used to purchase illicit or

age-restricted goods;

- applying identity fraud checks to ensure the customer is who they claim to be (Part 1 has further detail on this);
- applying enhanced monitoring to the customer relationship and individual transactions;
- establishing the source and /or the destination of funds.

Simplified customer due diligence

123. 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.

124. 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 to when a certain (low) monetary threshold is exceeded (whichever occurs first). The monetary threshold should not exceed EUR 250 where the product is not reloadable, can be used in other jurisdictions or for cross-border transactions or EUR 500 where it is permitted by national law. In this case, the product can only be used 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 with a EEA-regulated credit 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, e.g. 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 should not exceed EUR 250 for individual transactions or transactions that appear to be linked over the course of 12 months.

Chapter 4: Sectoral guidelines for money remitters

125. 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.

126. 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 might not themselves be obliged entities under applicable AML/CFT legislation; accordingly, their AML/CFT expertise may be limited.

127. 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 Service Businesses often carry out occasional transactions rather than establish a business relationship with their customers, which means that their understanding of the ML/TF risk associated with the customer may be limited.

128. 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

129. The following factors may indicate higher risk:

- the product allows high value or unlimited value transactions;
- the product or service have 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 senders in different countries to a local beneficiary.

130. The following factor may indicate lower risk:

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

Customer risk factors

131. The following factors may indicate higher 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 stay visible outside, or the customer reads instructions from a note;

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

  iv. the customer's transactions stay 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 set out in Article 5 of Regulation (EU) 2015/847. [18] Firms should note that Article 5(3)(a) of Regulation (EU) 2015/847prohibits the application of the EUR 1 000 threshold where a transaction is funded by cash or anonymous electronic money;

  v. the customer's use of the service is unusual, for example he sends or receives money to or from himself or sends 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, *e.g.* address or telephone number;

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

[18] 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).

132. The following factors may indicate lower 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 otherwise be increased.

Distribution channel risk factors

133. The following factors may indicate higher risk:

- there are no restrictions on the funding instrument, for example 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, for example the service is accessed entirely online;

- the money remittance service is provided through agents who:

  i. represent more than one principal;

  ii. have unusual turnover patterns compared to other agents in similar locations, *e.g.* unusually high transactions sizes, unusually large cash transactions, 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 high risk countries;

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

134. The following factors may indicate lower risk:

- agents are themselves regulated financial institutions;

- the service can only be funded by transfers from accounts held in the customer's name at an EEA credit or financial institution.

Country or geographic risk factors

135. The following factors may indicate higher risk:

- country of payer or payee is associated with high levels of criminal activity, such as terrorism, corruption, producing and/or trafficking of drugs and narcotics *etc.*;
- country of payee has no formal banking sector, which means that informal money remittance services, such as Hawala, may be used at point of payment.

Measures

136. Since many money remitters' business is primarily transaction-based, firms should consider which monitoring systems and controls they put in place to ensure they detect money-laundering and terrorist financing attempts even where the CDD information they hold on the customer is basic or missing.

137. 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; and
- systems to permit the establishment of the source of funds and the destination of funds.

138. 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

139. Money remitters using agents to provide payment services should know who their agents are.[19] As part of this, money remitters should establish and maintain appropriate and risk-sensitive policies and procedures for countering the risk that its agents may engage in, or be used for, money laundering or terrorist financing, including by:

[19] Article 17 of Directive 2007/64/EC.

- obtaining evidence 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 money laundering and terrorist financing 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 their own, and the agent's, AML/CFT compliance; and

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

Chapter 5: sectoral guidelines for wealth management

140. 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, tax and estate planning and associated facilities, including legal support.

141. 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.

142. 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 2 (retail banking), Chapter 7 (life insurance undertakings) and Chapter 9 (investment funds) may also be relevant in this context.

Risk factors

Product, service and transaction risk factors

143. The following factors may indicate higher risk:

- customers requesting large amounts of cash or other physical stores of value such as precious metals;
- very high value transactions;
- financial arrangements involving countries that are privacy havens or have a culture of banking secrecy;
- 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 identity 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 providers of financial services;
- assets deposited or managed in another financial institution, either of the same financial group or outside of the group, particularly abroad;
- the use of pooled or omnibus accounts, i.e. concentration accounts that are used to collect funds from a variety of sources for onward transmission.

Customer risk factors

144. The following factors may indicate higher risk:

- customers from high-risk countries associated with high levels of corruption, political instability, weak state institutions, weak anti-money laundering defences, armed conflict, widespread organised criminality, or a political economy dominated by oligopolistic actors with close links to the state;
- customers with income and/or wealth from high-risk sectors such as arms, extractive industries, construction, gambling, money service businesses, 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 with lifestyles that make it difficult to establish 'normal', or expected patterns of behaviour;
- customers whose identity evidence is of a non-standard form;
- very wealthy and influential clients, including customers with a high public profile, non-resident customers and PEPs. Where a customer or their beneficial owner are a politically exposed person, firms must always apply EDD in line with Articles 18 to 22 of Directive (EU) 2015/849.

Distribution channel risk factors

145. The following factor may indicate higher risk:

- the firm facilitates the customer being provided with a product or service by another

financial institution, which is not part of the same group as the firm.

Country or geographic risk factors

146. The following factors may indicate higher risk:

- business is conducted in countries that are privacy havens or have a culture of banking secrecy;
- the customer has relevant links to, or is from, a high risk jurisdiction, including jurisdictions identified by the Commission as having strategic AML/CFT deficiencies under Article 9 of Directive (EU) 2015/849;
- business is taking place in multiple countries.

Measures

147. The staff managing a wealth management firm's relationship with a customer (the relationship manager) should play a key role in assessing risk. This relationship manager's close contact with the customer will facilitate the collection of information that allows a fuller picture of the purpose and nature of the customer's business to be formed (for example, an understanding of the client's source of wealth, why complex or unusual arrangements may nonetheless be genuine and legitimate, or extra security may be appropriate). It 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 financial crime risks. As a consequence, independent oversight of risk assessment will also be appropriate, provided by, for example, the compliance department and senior management.

Enhanced customer due diligence

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

- obtaining and verifying more information about clients than in standard risk situations and review and, update this information on both a regular basis and when prompted by material changes to the clients' profile. Firms should perform this on a risk-sensitive basis, with review of higher-risk clients at least annually but more frequently if risk dictates. These procedures may include those for recording 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 increased 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, among others, by reference to:

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

ii. written confirmation of annual salary signed by employer;

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

iv. written confirmation of sale signed by advocate/solicitor;

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

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

vii. internet research 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, like retail banking or investment management;
- carrying out an independent internal review and appropriate senior management approval of all new clients and of 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 higher-risk jurisdictions.

  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 cash or other physical stores of value (such as travellers' cheques) are only handled at bank counters, and never by relationship managers;

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

Simplified customer due diligence

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

Chapter 6: Sectoral guidelines for trade finance providers

150. 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 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.

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

- 'open account' transactions. These are transactions where the buyer makes a payment once he has received the goods. These are the most common means of financing trade, but the underlying trade-related nature of the transaction will often not be known to the banks executing the fund transfer. Banks should refer to the guidance in Part 1 to manage the risk associated with such transactions;

- documentary Letters of Credit (LC). 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 (such as evidence that goods have been dispatched);

- documentary Bills for Collection (BC). 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 via their bank) to the importer in return.

152. Other trade finance products such as forfaiting or structured financing, or wider activity like project finance, are outside the scope of these sectoral guidelines. Banks offering these products should refer to the general guidelines in Title II. The guidelines on corporate finance may also be relevant in this context.

153. 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.

154. 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.[20] Banks should note that these standards do not have legal force and will not prevent banks from complying with their legal and regulatory AML/CTF obligations.

155. 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 (correspondent banking) may also be relevant in this context.

Risk factors

156. 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.

157. Banks should, nevertheless, use common sense and professional judgment to assess the extent to which the information and documentation they have could give rise to concern or suspicion of money laundering or terrorist financing.

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

Transaction risk factors

159. The following factors may indicate higher 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;
- use of copy documents in situations where original documentation would be expected, without reasonable explanation;
- significant discrepancies in documentation, for example between the description of goods in key documents (i.e. invoices and transport documents) and actual goods shipped;
- the type, quantity and value of goods is inconsistent with the bank's knowledge of the buyer's business;

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

- the goods transacted are higher risk for money-laundering purposes, for example certain commodities where prices can fluctuate significantly, which can make bogus prices difficult to detect; or require export licenses;

- 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, e.g. LCs are frequently amended without a clear rationale or goods are shipped through another jurisdiction for no apparent commercial reason.

160. The following factors may indicate lower risk:

- independent inspection agents have verified the quality and quantity of 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

161. The following factors may indicate higher 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 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 share 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.

162. The following factors may indicate lower 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 geographic risk factors

163. The following factors may indicate higher risk:

- a country associated with the transaction (including those where the goods originated from, are destined for, or transited through, or 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;

- countries associated with the transaction are high risk for money-laundering or terrorist financing purposes. This may include those with higher levels of predicate offences (such as those related to the narcotics trade, smuggling, counterfeiting) and free trade zones.

164. The following factors may indicate lower risk:

- the trade is within the EU/EEA;

- countries associated with the transaction have an AML/CTF regime comparable to that required under Directive (EU) 2015/849 and are associated with low levels of predicate offences.

Measures

165. 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 the bank has with the customer may assist its due diligence efforts.

166. 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.

167. 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

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

169. 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 these are based in a high-risk jurisdiction or handle high-risk goods. This may include checks of company registries, third-party intelligence sources, and open source internet searches;
- obtaining more information on the financial situation of the parties involved.

170. 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 legitimatel
- using professional judgment 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.

171. Since LCs and BCs are largely paper-based and accompanied by trade related documents (such as invoices and transport documents), 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 money laundering or terrorist financing. [21]

Simplified customer due diligence

172. 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.

[21] 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 anti- money laundering or counter-terrorist financing obligations.

Chapter 7: Sectoral guidelines for life insurance undertakings

173. Life insurance products are designed to financially protect the policyholder 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 is pooling the financial risks many different policyholders are faced with. Life insurance products can also be bought as investment products or for pension purposes.

174. 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 policyholder or a nominated or designated third party.

175. Most life assurance 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 from crime.

176. 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 (wealth management) and Chapter 9 (investment funds) may also be relevant in this context.

Risk factors

Product, service and transaction risk factors

177. The following factors may indicate higher risk:

- flexibility of payments, for example the product:
  - i. allows payments from third parties;
  - ii. allows high value or unlimited value premium payments, overpayments or large volumes of lower value premium payments;
  - iii. allows cash payments.
- ease of access to accumulated funds, for example the product:

i. allows partial withdrawals or early surrender at any time, with limited charges or fees;

ii. has a 'free look' [22] provision (these are sometimes known as 'cooling off periods').

- negotiability, for example the product:

  i. can be traded on a secondary market;

  ii. can be used as collateral for a loan.

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

178. The following factors may indicate lower risk:

The product

- only pays out against a pre-defined event, for example death, or on a specific date, such as 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;
- 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 such as pension schemes without early surrender option;
- cannot be used as collateral;
- does not allow cash payments;

[22] 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.

- has inflexible conditions that must be met to benefit from a tax relief.

Customer and beneficiary risk factors

179. The following factors may indicate higher 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 high corruption risk.
  vii. the contract is subscribed by a 'gatekeeper' such as fiduciary company, acting on behalf of the customer.
  viii. the policyholder and/or the beneficiary of the contract are companies with nominee shareholders and/or shares in bearer form.
- the customer's behavior:
  i. in relation to the contract, for example:
    a. the customer frequently transfers the contract to another insurer;
    b. frequent and unexplained surrenders, especially when the refund is done to different bank accounts;
    c. the customer makes frequent or unexpected use of 'free look' provisions/'cooling off' periods, in particular where the refund is made to an apparently unrelated third party;
    d. the customer incurs a high cost by seeking early termination of a product;
    e. the customer transfers the contract to an apparently unrelated third party;

f. the customer requests change or increase of the sum insured and/or of the premium payment.

ii. In relation to the beneficiary, for example:

a. the insurer is being 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.

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 which 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 third parties that are not associated with the contract;

f. catch-up contribution to a retirement plan close to retirement date.

180. The following factors may indicate lower risk:

In 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) which impose requirements to ensure adequate transparency of beneficial ownership, or is a majority-owned subsidiary of such a company;

- a public administration or a public enterprise from an EEA jurisdiction.

Distribution channel risk factors

181. The following factors may indicate higher risk:

- non-face-to-face sales, such as online, postal or telephone sales, without additional safeguards;
- long chains of intermediaries;
- intermediary is used in unusual circumstances (for example unexplained geographical distance).

182. The following factors may indicate lower 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 geographic risk factors

183. The following factors may indicate higher risk:

- the insurer, the customer, the beneficial owner, the beneficiary or the beneficial owner of the beneficiary are in different jurisdictions;
- the insurer, the customer, the beneficial owner, the beneficiary or the beneficial owner of the beneficiary are based in, or associated with, high risk jurisdictions, including those identified by the Commission as having strategic deficiencies in line with Article 9 of Directive (EU) 2015/849;
- premiums are paid through accounts held with financial institutions established in high risk jurisdictions, including those identified by the Commission as having strategic deficiencies in line with Article 9 of Directive (EU) 2015/849;
- the intermediary is based in, or associated with, high risk jurisdictions, including those identified by the Commission as having strategic deficiencies in line with Article 9 of Directive (EU) 2015/849.

184. The following factors may indicate lower risk:

- countries are identified by credible sources such as mutual evaluation or detailed assessment reports, as having effective AML/CFT systems;
- countries are identified by credible sources as having a low level of corruption, or

other criminal activity.

Measures

185. Article 13 (5) of Directive (EU) 2015/849 provides that for life insurance business, firms must not only apply CDD measures 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 arrangement are identified as the beneficiary; or

- obtain sufficient information to be satisfied that the identity 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.

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

187. 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

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

- where the customer makes use of the "free look"/"cooling off" period, refund the premium 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 raises suspicions about the transaction and whether submitting a suspicious activity report would be appropriate.

- taking additional steps 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 on the intended nature of the business relationship in order to establish this intended nature;

iv. obtaining additional information on the customer and updating more regularly the identification data of 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 wait until they are identified or designated;

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

x. in line with Article 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 in line with those required under Directive (EU) 2015/849.

- Article 20 of Directive (EU) 2015/849 requires that where the risk associated with a PEP relationship is increased, firms must not only apply CDD measures in line with Article 13, AMLD, 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;

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

Simplified customer due diligence

189. The following measures may satisfy some of the CDD requirements in very 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 in the sole or joint name of the customer with a 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 managers

190. 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 the customers' behalf.

191. 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.

192. 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 (wealth management) may also be relevant in this context.

Risk factors

Product, service or transaction risk factors

193. The following factors may indicate higher risk:

- transactions are unusually large;
- third party payments are possible;

Customer or investor risk factors

194. The following factors may indicate higher risk:

- the customer's behavior, for example:
    i. repurchasing or redeeming a long-term investment within a short period after the initial investment or before the payout date, in particular where this results in financial loss or payment of high transaction fees;

ii. the repeated purchase and sale of shares within a short period of time without an obvious strategy or economic rationale;

iii. refusal or unwillingness to provide CDD information;

iv. frequent changes to CDD information or payment details;

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

vi. the circumstances in which the customer makes use of the "cooling off" period gives rise to suspicion;

vii. using multiple accounts without previous notification, especially when these accounts are held in multiple or high risk jurisdictions.

- the customer 's nature, for example:

  i. the customer is an offshore company or trust;

  ii. the customer is an unregulated fund who carries out little or no due diligence on its underlying investors;

  iii. the customer is an unregulated third party investment vehicle, for example a hedge fund;

  iv. the customer's ownership and control structure is opaque;

  v. the customer is a PEP or otherwise influential individual.

- the customer's business, for example he customer's funds are derived from business in sectors that are associated with higher financial crime risk.

195. The following factors may indicate lower risk:

- the customer is an institutional investor whose status has been verified by an EEA government agency, e.g. a government-approved pensions scheme;

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

Country or geographic risk factors

196. The following factors may indicate higher risk:

- the investor or their custodian is based in a high risk jurisdiction, including off-shore jurisdictions;

- the funds come from a high risk jurisdiction, including off-shore jurisdictions.

Measures

197. Investment managers typically need to develop a good understanding of their customer, their customer's circumstances and anticipated levels of transactions to help them identify suitable investment portfolios. This information will be similar to that firms will obtain for AML/CFT purposes.

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

- identify and, where necessary, verify the identity of underlying investors 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, in particular where the firm provides custody services.

199. To the extent permitted by national legislation, investment managers may apply the guidelines on SDD in Title II in low risk situations.

Chapter 9: Sectoral guidelines for providers of investment funds

200. The provision of investment funds can involve multiple parties, such as the management company, depositary bank, registrars, platforms, investment managers and financial advisors. The type and number of parties involved in the provision of investment funds depends on the nature of the investment and will affect how much the firm knows about their customer and investors.

201. Investment funds can be abused for ML/TF purposes. Retail funds are often conducted on a non-face to face basis; access to such funds is often easy and holdings of investment funds can easily be transferred between different parties. However, the medium- to long term nature of the investment can contribute to limiting the attractiveness of these products for money launderers. Institutional funds are exposed to similar risks, though these risks may be reduced where such funds are open only to a small number of investors.

202. 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 7 (life insurance undertakings) and Title III Chapter 8 (investment management) may also be relevant in this context.

Risk factors

Product, service or transaction risk factors

203. The following factors may indicate higher risk:

- the transaction involves third party subscribers or payees, in particular where this is unexpected;
- the transaction involves accounts or third parties in multiple jurisdictions, in particular where these jurisdictions are associated with a high ML/TF risk.

204. The following factor may indicate lower risk:

- third party payments are not allowed.

Customer or investor risk factors

205. The following factors may indicate higher risk:

- the customer or investor's behavior, for example:

  i. repurchasing or redeeming a long-term investment within a short period after the initial investment or before the payout date, in particular where this results in financial loss or payment of high transaction fees;

  ii. the repeated purchase and sale of shares within a short period of time without an obvious strategy or economic rationale;

  iii. refusal or unwillingness to provide CDD information;

  iv. frequent changes to CDD information or payment details;

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

  vi. the circumstances in which the customer makes use of the "cooling off" period gives rise to suspicion;

  vii. using multiple accounts without previous notification, especially when these accounts are held in multiple or high risk jurisdictions;

  viii. sudden change in clearing and settlement location without rationale related to any change in the country residence of the client.

- the customer or investor's nature, for example making investments that are inconsistent with the customer's nature or overall financial situation.

206. The following factors may indicate lower risk:

- the customer is an institutional investor whose status has been verified by an EEA government agency, e.g. a government-approved pensions scheme;

- the customer or investor is a regulated financial intermediary in an EEA country.

Distribution channel risk factors

207. The following factors may indicate higher risk:

- the fund admits a wide, or unrestricted, range of investors;

- multiple relationships, which limits firms' oversight of its business relationships and restricts their ability to monitor transactions.

208. The following factors may indicate lower risk:

- the fund admits only a specific type of low-risk investors;
- the fund can be accessed only through regulated financial intermediaries in EEA countries, who are within scope of their national AML/CFT legislation.

Country or geographic risk factors

209. The following factor may indicate higher risk:

- investors' funds have been generated in high risk jurisdictions, in particular those associated with higher levels of predicate offences to money laundering.

Measures

Enhanced customer due diligence

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

- obtaining additional customer information during identification, such as occupation, level of assets, information available in public databases, the Internet, background and business objectives, information on the reasons for the proposed transactions;
- taking additional steps to verify the documents obtained;
- obtaining information on the source of funds and/or the customer's financial assets;
- tequiring that the redemption payment is made through the initial account used for investment;
- establishing limits on number and/or amount of transactions;
- requiring that the first payment is made through an account in the name of the customer with a bank subject to equivalent AML/CFT standards;
- obtaining approval from senior management at the time of the transaction when a customer uses a product or service for the first time;
- applying enhanced monitoring of the customer relationship and individual transactions;
- using anti-impersonation fraud checks to mitigate the risk of impersonation fraud

where the relationship is conducted on a non-face to face basis. Examples include sending a letter to the customer's address or applying additional verification measures (such as checking against online databases) to verify the existence of the purported identity.

Simplified customer due diligence

211. To the extent permitted by national legislation and provided that the funds are being transferred to or from an account held in the customer's name at an EEA credit institution, examples of SDD measures firms may apply include using the source of funds or the destination of funds to meet some of the CDD requirements.

Intermediaries

212. Where a firm uses a financial intermediary to distribute fund shares, for example a regulated platform, a bank or a financial adviser, that intermediary may be regarded as the firm's customer provided that the intermediary acts on its own account as the direct counterparty of the firm. This could be the case, for example, where the intermediary receives from its customer a mandate to manage their assets or carry out one or more investment transactions. In those situations, the firm should treat the intermediary's customers as the fund's beneficial owners.

213. In those situations, the firm may apply SDD measures provided that:

- the financial intermediary is subject to AML/CFT obligations in an EEA jurisdiction;
- the ML/TF risk associated with the business relationship is low, based on the firm'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, among others; and
- the firm is satisfied that the intermediary applies robust and risk-sensitive CDD measures to their own clients and their clients' beneficial owners. It may be appropriate for the firm to take risk-sensitive measures to assess the adequacy of its intermediary's CDD policies and procedures, for example by referring to publicly available information about the intermediary's compliance record, liaising directly with the intermediary or by sample-testing the intermediary's ability to provide CDD information upon request.

214. Where those conditions are met, and subject to applicable national legislation permitting this, SDD may consist of the firm:

- identifying and verifying the identity of its intermediary, including the intermediary's beneficial owners;

- assessing the purpose and intended nature of the business relationship;
- conducting ongoing monitoring of the business relationship; and
- establishing that the intermediary will provide upon request relevant information on their clients, who invested in the fund and who are the fund's beneficial owners.

215. Where the financial intermediary is established in a third country, or where there are indications that the risk associated with the business relationship may not be low, firms should apply full CDD, including reliance as per Article 25 of Directive (EU) 2015/849 or EDD measures as appropriate.

Title IV - Implementation

Implementation

216. Competent authorities and firms should comply with these guidelines by the earlier of the following dates:

- 26 June 2017;
- the date on which the Member State of the relevant competent authorities brings into force the laws, regulations and administrative provisions necessary for it to comply with Directive (EU) 2015/849.

5. Accompanying documents

5.1. Impact Assessment

Introduction

1. Directive (EU) 2015/849 (the anti-money laundering Directive, AMLD) places the risk-based approach at the centre of the Union's anti-money laundering and counter terrorist financing (AML/CFT) regime. It makes clear that the risk of money laundering and terrorist financing (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 European Supervisory Authorities (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 customer due diligence 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 different 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 AMLD. They found that the application of these guidelines would not give rise to significant costs over and above those 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 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 from the full implementation of the proposed guidelines'; the impact from 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 simplified customer due diligence 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 enhanced customer due diligence 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 money laundering and terrorist financing risk factors or simplified and enhanced due diligence so far. However, relevant guidance has been published by international standard-setters, including the Financial Action Task Force and the Basel Committee for Banking Supervision.

Option 1

11. The ESAs' guidelines could copy out, or simply refer to, international standards and guidance on ML/TF risk factors and simplified and enhanced customer due diligence.

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 in Articles 17 and 18(4) of Directive (EU) 2015/849. This is because international guidance does not

    - take into account specific measures foreseen in Directive (EU) 2015/849, for example in relation to certain electronic money products or high risk-jurisdictions 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; and
    - 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 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.

20. Option 2 is the ESAs' preferred option because it allows firms and competent authorities to comply with international standards and guidelines on the one hand, while at the same time 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 customer due diligence, 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 Due Diligence.

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 separate guidelines on high and low risk respectively.

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.

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 supervisory expectations.

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

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 or 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 which could move a business relationship or occasional transaction into a higher or lower risk category. For example, setting monetary thresholds at European level below which a relationship should be considered low risk 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 have not already been set out in 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 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 risks effectively.

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 option are guidelines that

- Are consistent with relevant international standards and guidance;
- Address both high and low risk factors;
- Combine generic 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 approach to comply with a new nation legal framework 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 to review their own internal policies and controls, make necessary adjustments to reflect these guidelines and to train 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; and since these adjustments are likely to take place at the same time as new legislation to transpose Directive (EU) 2015/849 will 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 of costs and benefits 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 these 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 customer due diligence.

58. The cost to competent authorities will arise mainly from a review of existing regulatory guidance to firms and supervisory manuals to ensure consistency with these guidelines. Competent authorities will also incur some costs to retrain 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 are unlikely to exceed the costs arising from the implementation of national legislation that transposes Directive (EU) 2015/849.

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

5.2. 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.