cssf

Commission de Surveillance
du Secteur Financier

Circular CSSF 21/782

Adoption of the revised guidelines, by EBA, on money laundering and terrorist financing risk factors

Commission de Surveillance du Secteur Financier

Circular CSSF 21/782

Concern: Adoption of the revised guidelines, by EBA, on money laundering and terrorist financing risk factors

Luxembourg, 24 September 2021

Dear Madam, dear Sir,

The purpose of this circular is to draw your attention to the adoption by the European Banking Authority ("EBA") of the **Revised** Guidelines on customer due diligence and the factors credit and financial institutions ("the professionals") should consider when assessing the money laundering and terrorist financing ("ML/TF") risk associated with individual business relationships and occasional transactions ("the Guidelines") under Articles 17 and 18(4) of Directive (EU) 2015/849 of the European Parliament and of the Council of 20 May 2015 on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing, amending Regulation (EU) No 648/2012 of the European Parliament and of the Council, and repealing Directive 2005/60/EC of the European Parliament and of the Council and Commission Directive 2006/70/EC1.

Since the publication of the original Joint Guidelines of the three European Supervisory Authorities (EBA, ESMA, EIOPA, i.e. "ESAs") in 2017, Directive (EU) 2018/843 (5AMLD) amending Directive (EU) 2015/849, entered into force on 9 July 2018. The applicable legislative framework in the EU has thus changed and simultaneously, new ML/TF risks have emerged.

For instance, the ESAs' 2019 Joint Opinion on the ML/TF risks affecting the EU's financial sector highlighted ongoing concerns by competent authorities across the EU, about professionals' identification and assessment of both the business-wide risk and the risks associated with individual business relationships, and about the application of relevant CDD measures.

Thus, so as to ensure the ongoing relevance and accuracy of the Guidelines, and to support the professionals' AML/CFT compliance efforts, the Guidelines have been updated and completed accordingly. The revision of the Guidelines was also used as an opportunity to make further editorial amendments and to improve consistency throughout the document.

The purpose of the Guidelines continues to provide guidance on the different ML/TF factors the professionals should consider when assessing their risks. Moreover, the Guidelines also specify how the professionals can adjust anti-money laundering and counter-terrorist financing ("AML/CTF") customer due diligence measures commensurate with the level of risk associated with a business relationship or occasional transaction. Thus, they set out examples of due diligence measures, either simplified for lower risk or enhanced in order to mitigate higher identified risks.

These revised Guidelines take account of the new and emerging risks related for example with the use of RegTech solutions for CDD purposes or terrorist financing, and contains more guidance on the identification of beneficial owners and enhanced customer due diligence related to high-risk third countries.

Moreover, the Guidelines stress that professionals enhance in particular their understanding of (risks related to) tax crimes as there are substantial similarities between the techniques used to launder the proceeds of crimes and to commit tax crimes. Professionals should notably consider other relevant reports of EBA and/or ESMA, particularly the reports[1] and Action plan[2] on dividend arbitrage trading schemes ('Cum-Ex/Cum-Cum schemes').

Finally, the Guidelines also specify that an effective risk-based approach should not result in systematically exiting or discontinuing to offer services to certain categories of customers associated with higher ML/TF risk ("de-risking" approach) and that professionals should also carefully balance the need for financial inclusion with the need to mitigate ML/TF risk.

While the original Guidelines are replaced by the revised Guidelines, the structure of the Guidelines has remained the same.

The first part of the Guidelines (Title II) provides information on the general application of due diligence. More detailed information on sector-specific risk factors and the relevant due diligence measures are set out in the second part (Title III). The following sectors continue to be covered in Title III:

- Correspondent banking relationships;
- Retail banking;
- Electronic money issuers;
- Money remitters;
- Wealth management;
- Trade finance providers;
- Life insurance undertakings;
- Investment firms;
- Providers of investment funds.

However, additional (new) sectoral guidelines have been added in Title III on the following topics:

- Crowdfunding platforms;
- Providers of currency exchange services;
- Corporate finance;

[1] *Esma70-155-10272_final_report_on_cum_ex_and_other_multiple_withholding_tax_reclaim_schemes.pdf (europa.eu)*

[2] *Action plan on dividend arbitrage trading schemes Cum-ExCum-Cum.pdf (europa.eu)*

- Payment initiation services providers (PISPs);
- Account information service providers (AISPs).

In particular, concerning the last two new sections in relation to AISPs and PISPs, it should be noted that while those providers qualify as obliged entities under EU law, the Guidelines acknowledge that the inherent ML/TF risk associated with AISPs and PIPS is limited and that therefore simplified due diligence measures are appropriate in most situations.

As to the scope of application of the Guidelines, professionals need to apply the changes to future business relationships and also to existing customers at appropriate times as risk assessment and mitigation is an ongoing process and professionals must make sure that any new controls apply to both categories of customers (existing and new).

It must be noted that neither the risk factors nor the due diligence measures described in the Guidelines are to be considered as exhaustive.

Based on the Guidelines, the professionals should be able to take informed decisions commensurate with the ML/TF risks in order to efficiently manage their business relationships and occasional transactions, by taking into account supervisory expectations as regards the manner in which important AML/CTF obligations should be fulfilled.

The Guidelines are applicable as of 26 October 2021.

The Guidelines are annexed to this circular. They are also available on the websites of the European Supervisory Authorities, as for example on the EBA's website at:

https://www.eba.europa.eu/sites/default/documents/files/document_library/Publications/Guidelines/2021/963637/Final%20Report%20on%20Guidelines%20on%20revised%20ML%20TF%20Risk%20Factors.pdf

This circular repeals and replaces circular CSSF 17/661.

Claude WAMPACH
Director

Marco ZWICK
Director

Jean-Pierre FABER
Director

Françoise KAUTHEN
Director

Claude MARX
Director General

Annex

EBA/GL/2021/02

1 March 2021

Final Report

Guidelines

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

Contents

1. Executive summary

On 26 June 2015, Directive (EU) 2015/849 on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing (ML/TF) entered into force. It recognised that the risk of ML/TF can vary and that Member States, competent authorities and obliged entities have to take steps to identify and assess that risk with a view to deciding how best to manage it. It also required the European Supervisory Authorities (ESAs) to issue guidelines on key aspects of the risk-based approach. In June 2017, the three ESAs issued Guidelines on risk factors and simplified and enhanced customer due diligence (JC 2017 37). These guidelines set out factors firms should consider when assessing the ML/TF risk associated with a business relationship or occasional transaction. They also set out how firms can adjust the extent of their customer due diligence measures in a way that is commensurate to the ML/TF risks they have identified.

Since then, the applicable legislative framework in the EU has changed, and new risks have emerged. On 9 July 2018, Directive (EU) 2018/843 entered into force. This directive amended Directive (EU) 2015/849 and introduced a number of changes that warranted a review of the Risk Factors Guidelines to ensure their ongoing accuracy and relevance; this was the case in particular in relation to the provisions on enhanced customer due diligence related to high-risk third countries.

Furthermore, the ESAs' 2019 Joint Opinions on the ML/TF risk affecting the EU's financial sector highlighted ongoing concerns, by competent authorities across the EU, about firms' identification and assessment of both business-wide risk and the risk associated with individual business relationships, and the application of CDD measures.

To support firms' AML/CFT compliance efforts and enhance the ability of the EU's financial sector effectively to deter and detect ML/TF, these guidelines have been updated regarding:

- business-wide and individual ML/TF risk assessments;
- customer due diligence measures including on the beneficial owner;
- terrorist financing risk factors; and
- new guidance on emerging risks, such as the use of innovative solutions for CDD purposes.

As was the case previously, these Guidelines are divided into two parts:

Title I 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 ML/TF risk associated with individual business relationships or occasional transactions.

Title II is sector-specific and complements the generic guidelines in Title I. It sets out risk factors that are of particular importance in certain of those sectors and provides guidance on the risk-sensitive application of Customer Due Diligence measures by firms in those sectors. So as to foster greater convergence of supervisory expectations of the measures firms should take to tackle emerging risks, additional sectoral guidelines have been added to the original Risk Factors Guidelines on crowdfunding platforms, providers of currency exchange services, corporate finance, and payment initiation services providers (PISPs) and account information service providers (AISPs). Therefore, in total Title II now contains thirteen sectoral guidelines about very different key financial sectors such as for instance correspondents banking, retail banking, electronic money, money remittance, life insurance and investments firms.

Together, Title I and Title II 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. Importantly, neither these guidelines nor the Directive's risk-based approach require the wholesale exiting of entire categories of customers irrespective of the ML/TF risk associated with individual business relationships or occasional transactions.

Since 1 January 2020, following changes to Regulation (EU) No 1093/2010 by Regulation (EU) 2019/2175, the EBA has been solely responsible for leading, coordinating and monitoring AML/CFT efforts across the entire EU financial sector. In 2019, the European legislature consolidated the AML/CFT mandates of all three ESAs within the EBA. According to Articles 17 and 18(4) of Directive (EU) 2015/849 as amended by Directive (EU) 2019/2177, the EBA is mandated to issue the ML/TF Risk Factors Guidelines and it was the EBA only that publicly consulted on a version of these guidelines between 5 February 2020 and 6 July 2020. The EBA held a public hearing on 15 May 2020. The Consultation Pape (JC 2019 87) attracted 58 responses from a wide range of stakeholders across sectors covered by these Guidelines. The EBA published the responses on its website on 4 August 2020. The EBA has reviewed and assessed the responses it received and brought changes to the guidelines where appropriate and necessary.

This report also explains where the EBA:

- agreed with some of the proposals made by respondents and made changes to the draft Guidelines as a result, e.g. with regard to Account Information Service Providers and Payment Initiation Service Providers in Guideline 18;

- saw the need to provide additional clarity on the interpretation of new or amended Guidelines, in some of the cases where respondent requested this; and

- considered it relevant for respondents to become aware of other work that the EBA is pursuing (e.g. on financial inclusion and the Action plan on dividend arbitrage trading schemes ('Cum-Ex/Cum-Cum')) that may be more relevant to them in the context of their questions.

Next steps

The guidelines will be translated into the official EU languages and published on the EBA website.

The deadline for competent authorities to report whether they comply with the guidelines will be two months after the publication of the translations.

The guidelines will apply three months after publication in all EU official languages.

Upon the date of application, the original guidelines (JC/2017/37) will be repealed and replaced with the revised guidelines.

2. Abbreviations

AISP	Account Initiation Service Provider
AML	Anti-money laundering
BCs	Bills for collection
CDD	Customer due diligence
CFT	Countering the financing of terrorism
CSP	crowdfunding service provider
EBA	European Banking Authority
EDD	Enhanced customer due diligence
ESAs	European Supervisory Authorities
FATF	Financial Action Task Force
FIU	Financial Intelligence Unit
FRSBs	FATF-style Regional Bodies
FSAP	Financial Sector Assessment Programme
GDPR	General Data Protection Regulation
ICC	International Chamber of Commerce
IMF	International Monetary Fund
LCs	Letter of Credits
NRA	National Risk Assessment
OECD	Organisation for Economic Co-operation and Development
PEP	Politically Exposed Person
PISP	Payment Initiation Service Provider
RMA	Risk Management Application
SDD	Simplified customer due diligence
SNRA	Supra National Risk Assessment
SSPE	Securitisation Special Purpose Entity

3. Background and rationale

3.1 Background

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

2. Article 17 and 18(4) of Directive (EU) 2015/849 required 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[1]. The aim was 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.

3. In June 2017, the three ESAs issued Guidelines on risk factors and simplified and enhanced customer due diligence (JC/2017/37). 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.

4. Since the publication of the original Guidelines, Directive (EU) 2018/843 (AMLD5) entered into force on 9 July 2018. AMLD5 introduced a number of changes that warranted a review of the guidelines to ensure their ongoing accuracy and relevance. This was the case in particular in relation to the provisions on enhanced customer due diligence related to high-risk third countries.

5. Furthermore, the ESAs' Joint Opinions on the ML/TF risk affecting the EU's financial sector, published in 2017 and 2019, highlighted ongoing concerns, by competent authorities across the EU, about firms' identification and assessment of both, business-wide risk and the risk associated with individual business relationships, and the application of CDD measures. These new guidelines take account of new and emerging risks, for example the use of RegTech solutions for CDD purposes, terrorist financing risk factors, and contains guidance on customer due diligence measures (including guidance on the identification of beneficial owners).

[1] Annexes II and III of Directive (EU) 2015/849 provides a non-exhaustive list of factors of potentially lower or higher risk that obliged entities should at least take into account when assessing the risks of money laundering and terrorist financing. Article 16 and Article 18(3) of Directive (EU) 2015/849.

6. The ESAs therefore decided to update the guidelines to ensure their ongoing relevance and accuracy, and to further 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 firms should apply it. The guidelines will help firms identify, assess and manage the ML/TF risk associated with their business, and with individual business relationships and occasional transactions in a risk-based, proportionate and effective way.

7. Since 1 January 2020, following changes to Regulation (EU) No 1093/2010 by Regulation (EU) 2019/2175, the EBA has been solely responsible for leading, coordinating and monitoring AML/CFT efforts across the entire EU financial sector. In 2019, the European legislature consolidated the AML/CFT mandates of all three ESAs within the EBA. Pursuant to Articles 17 and 18(4) of Directive (EU) 2015/849 as amended by Directive (EU) 2019/2177, since 1 January 2020 the EBA has been mandated to issue the ML/TF Risk Factors Guidelines, and it was the EBA only that publicly consulted on a version of these guidelines between 5 February 2020 and 6 July 2020. A public hearing took place on 15 May 2020.

8. The Consultation Paper (JC 2019 87) included a number of specific questions for respondents to consider (which are reproduced in Chapter 4.1 of this report). The EBA received 58 responses. The responses were submitted by a wide range of financial sector participants, including supervisory authorities, credit institutions, payment institutions, payment initiation service providers, account information service providers, electronic money institutions, investment firms, life insurance undertakings, employee representative organizations, and several industry organizations and consultancy/advisory firms.

9. The Feedback Table in Chapter 4.3 provides a complete list of all consultation responses received by the EBA, with the EBA's assessment, as well as any changes that the EBA decided to make to the Guidelines as a result, where applicable.

10. The original guidelines will be repealed and replaced with the revised guidelines.

3.2 Rationale

11. The consultation was limited to changes made in the original version of the Guidelines, that address changes to firms' obligations as a result of the new EU legislative framework and new risks, and that clarify regulatory expectations in those areas where evidence suggested that divergent approaches continued to exist. The scope of the consultation, and of the consultation questions, therefore did not include provisions that the ESAs have left unchanged and that had already been consulted on during the development of the original Guidelines.

12. This section sets out the EBA's view on the consultation responses received that:

    - warrant material changes in the Guidelines (e.g. on Account information and payment initiation service providers, Guideline 18);

- do not seek a change in the Guidelines, but where the EBA sees the need to provide additional context on the interpretation of new provisions in the Guidelines; and

- link to other work that the EBA is pursuing.

Business-wide risk assessments

13. Several respondents raised questions relating to business-wide risk assessments. Some respondents queried whether firms should take a 'holistic view' on ML/TF risks only for individual risk assessments, or as a general principle. By way of feedback, the EBA notes that Guideline 1.26 states that firms should take a holistic view of individual risk assessments, while AMLD in recital 22 refers to a holistic, risk-based approach for all ML/TF risks in the sense of comprehensive risk-based methods and monitoring approaches, not only at individual level but also at business-wide level. The EBA has therefore decided to amend Guideline 1.12 by making it explicit that the holistic approach should also be applied in the business-wide risk assessment.

14. Some other respondents asked which risk factors should be considered when a firm puts into place systems and controls to identify emerging risks for the business-wide risk assessment. In its assessment, the EBA acknowledged that firms should consider the full range of risk factors, including products and services, the jurisdictions they operate in, the (categories of) customers they attract (particularly the high risk category) and the distribution channels they use. The EBA has therefore made the Guideline 1.9. b) ii) c) more consistent with the principles of AMLD and Guideline 1.12.

Non-face-to-face interactions

15. Many respondents raised questions on non-face-to-face interactions, a topic that gained more relevance since the COVID-19 pandemic and associated restrictions on movement, and the resulting increased use of new technology for identification and verification purposes.

16. For example, some respondents asked the EBA how far firms should go to assess the risk that the customer may have sought to avoid face-to-face contact deliberately for reasons other than convenience or incapacity (Guideline 2.21 a) i). The EBA has assessed the responses and has decided to simplify Guideline 2.21 a) i) by removing such requirement, as the EBA considers that the key risk and its mitigation are already captured sufficiently by sub ii) and sub iii) that require the firm to consider whether the firm used a reliable form of non-face-to-face CDD and has taken steps to prevent impersonation or identity fraud. Where the risk associated with a non-face to face relationship or an occasional transaction is increased, firms should apply EDD measures in line with Guideline 4.30.

17. Other respondents queried which forms of technology are deemed reliable. The EBA notes that Guideline 4.31 already stated that the use of electronic means of identification does not, in itself, give rise to increased ML/TF risk, in particular where these electronic means provide

a high level of assurance under Regulation (EU) 910/2014. Firms should apply Guidelines 4.32 to 4.37 when using innovative technological means to verify identity.

18. That said, in relation to innovative solutions, the EBA has decided to update Guideline 4.33 so as to better consider ICT and security risks and align the wording with the final Guidelines on ICT and security risk management (EBA/GL/2019/04).

19. Lastly, the EBA notes that the European Commission recently invited the EBA to draft guidelines, in 2021, on elements related to customer remote on-boarding and reliance on customer due diligence processes carried out by third parties. The EBA will publish draft requirements for public consultation in due course.

Account information and payment initiation services

20. The sector-specific Guideline 18 on Account Information Service Providers (AISPs) and Payment Initiation Service Providers (PISPs) received the largest number of responses. Some respondents asked the EBA to consider whether AISPs and PISPs are obliged entities under the AMLD. The EBA highlights that EU law defines AISPs and PISPs as obliged entities, more specifically under Article 2 AMLD. The EBA recently provided advice to the European Commission (EC) on a future EU AML/CFT framework (EBA/OP/2020/14 and EBA/REP/2020/25), recommending to the EC to further assess the inclusion of AISPs as obliged entities.

21. Other respondents queried whether there is room for more proportionality in the Guidelines. The EBA notes that in the Guidelines, the EBA acknowledged that the inherent ML/TF risk associated with AISPs and PISPs is limited and that therefore simplified due diligence (SDD) measures are appropriate in most situations. The EBA did however see room to make the Guidelines more proportionate, by:

- Further differentiating between the different business models of AISPs and PISPs. For example, the definition of the customer from the PISP's perspective in Guideline 18.8 a) has been amended, in order to confirm that PISPs should assess whether they have a business relationship in the meaning of Article 3(13) of the AMLD with the payer and/or with the payee, and other circumstances set out in Article 11 AMLD, in order to conclude who the customer is, and, more specifically, to emphasize that PISPs do not always enter into a business relationship in the meaning of Article 3(13) of the AMLD with the payer.

- Providing additional clarification on risk factors (Guidelines 18.4 and 18.6) that AISPs and PISPs should take into account. The risk factors have been streamlined, including by further differentiating between aspects relevant AISPs or PISPs respectively; and

- Explicitly reflecting the data sets available to AISPs and PISPs (Guidelines 18.9, 18.10 and 18.11). The EBA confirms that AISPs and PISPs should take all available information into account. Where data that might be of importance for AML/CFT purposes is not available to

AISPs and PISPs in the context of PSD2, the Guidelines do not require that AISPs and PISPs pro-actively request such information.

Trade financing

22. Several respondents queried a provision related to trade financing, in particular the transaction risk factor that refers to goods traded to 'prohibited end users'. Guideline 13.10(l) includes a risk factor that traded goods are destined to an embargoed country, to a prohibited end user, or in support of a prohibited end-user. The EBA has made editorial changes to clarify this relates to goods that are destined to parties or countries that are under sanctions, embargos or similar measures issued by, for example, the Union or the United Nations or in support of such party or country, similar to what is provided in Annex III 3(c) AMLD. Depending on the circumstances and assessment of risk, firms may also decide not to pursue such transactions.

Crowdfunding

23. After the consultation paper was published, Regulation (EU) 2020/1503 on European crowdfunding service providers for business has been published. The EBA has amended Guideline 17.1 in order to reflect the relevant definitions provided in that Regulation. The EBA has also clarified that Guideline 17 refers to 'customers' in the meaning of 'clients', as defined in Regulation (EU) 2020/1503. Furthermore, the EBA has removed the redundant Guideline 17.13.

Editorial amendments

24. Many of the comments made by respondents required small editorial or no changes. The EBA has used the opportunity of the revision of these Guidelines to make further editorial amendments, and to improve consistency throughout the Guidelines further to suggestions made, e.g. to streamline the treatment of listed companies (Guidelines 13.3, 14.9, 15.6, 20.5), the reference to 'electronic identification means' (Guideline 9.10, 10.8, 14.10 and 17.7), the use of 'opaque' structures (Guideline 2(d), 4.15 and 9.6(a) vii and Guideline 20)) and the use of 'non-cooperative jurisdiction for tax purposes' (Guideline 13.14 b). Furthermore, references to legislation were updated or wording aligned (e.g. on training in Guideline 6.2, removal of 'beneficiary' in Guideline 14.16, addition of 'customer' in Guideline 16.13, 'resident in' in Guideline 4.56, 'MIFID II' in Guideline 15.1 and 15.9 and several footnotes removed or updated.

High-risk third countries

25. Another topic that attracted many responses is the inclusion of provisions on high-risk third countries in the new Guidelines 4.53-4.57. Several respondents expressed the view that the definition of what should be considered a business relationship or a transaction involving a high-risk country was too broad, and that firms may have limited knowledge of criteria specified in the Guidelines. They suggested to align the wording with AMLD provisions and to

ensure flexibility, which would also allow firms to take into account additional information when assessing business relationships and transactions involving high-risk third counties.

26. By way of feedback, the EBA notes that the AMLD requires specific EDD measures to be applied to business relationships and transactions involving high-risk third countries as set out in Article 9(2) of AMLD. Consequently, Guideline 4.53 refers to such business relationships and transactions where firms should ensure that they apply at a minimum the EDD measures set out in Article 18a (1) and, where applicable, the measures set out in Article 18a (2) of AMLD. The EBA, having consulted with the European Commission and national competent authorities prior to the publication of the CP, has explained in Guidelines 4.55 to 4.57 what 'involving high risk third countries' means. The EBA also included a list of key elements that all firms should assess as a minimum, whereby firms are free to also consider additional aspects as they deem fit. Having assessed the consultation responses, the EBA has made editorial amendments in Guideline 4.53, 4.56 and 4.57. In this context, the EBA has also amended Guidelines 12.7 and 12.8 to reflect this assessment with regards to the destination of funds.

Financial inclusion and de-risking

27. Several respondents indicated that they found it challenging to comply with AML/CFT requirements and ensure financial inclusion at the same time and queried how to implement this in practice. By way of feedback, the EBA notes that it has introduced three new Guidelines (4.9 to 4.11) in the CP, requiring firms to apply risk sensitive measures, through which more individuals and businesses, especially low-income, unserved and underserved groups, should be able to get access and use regulated financial services, which could in turn, actually increase the effectiveness of the fight against ML/TF. The EBA has added a sentence on de-risking to make it clearerthat the Guidelines do not require firms to no longer offer services to some categories of customers associated with higher ML/TF risk. As the risk associated with individual business relationships will vary, even within one category, the application of a risk-based approach does not require firms to refuse, or terminate, business relationships with entire categories of customers that are considered to present higher ML/TF risk. Firms should carefully balance the need for financial inclusion with the need to mitigate ML/TF risk.

28. The EBA also notes that the Guidelines do not prevent firms from establishing a correspondent banking relationship with a respondent situated in a high-risk third country, provided that the risk is mitigated through enhanced due diligence measures. The EBA specifies in GL 4.10 b) that firms should ensure that their approach to applying CDD measures does not result in unduly denying legitimate customers access to financial services. Therefore, the key focus of firms should be on policies and controls that are commensurate to the risks identified.

29. At the same time, the EBA sees the need to better understand not only the scale and drivers of exacerbating financial exclusion but also the wider issue of 'de-risking' and its impact on individual consumers and legal entities. The EBA therefore launched a separate Call for Input in 2020, to understand why financial institutions choose to de-risk and therefore exacerbate financial exclusion, instead of managing the risks associated with certain sectors or categories

of customers. The Call for Input has received more than 300 responses by the deadline in September 2020 and the EBA is currently assessing the implications for its policy development in this area. The feedback gathered from this Call will feed into the EBA's next Opinion on the risks of money laundering and terrorist financing affecting the Union's financial sector that the EBA is mandated to issue under Article 6(5) of the AMLD and potentially other EBA outputs.

Scope of application of the Guidelines

30. A number of respondents sought clarification with regard to the application of the Guidelines, in particular whether the changes apply only to new business relationships, or also to existing business relationships and by when firms should comply with the new requirements.

31. By way of feedback, the EBA notes that pursuant to Article 14(5) AMLD, firms need to apply CDD measures also to existing customers at appropriate times on a risk sensitive basis, or when circumstances change. Moreover, the revised Guidelines already make explicit that risk assessment and mitigation is an ongoing process and that firms must make sure that any new controls apply to new customers as they apply to existing customers.

Independent reviews

32. The newly introduced Guideline 7.2 states that firms should consider whether an independent review of their approach may be warranted or required. Respondents asked what is meant by 'independent review', on what basis it is required, how it should be performed (internal or external, on part of the processes and controls or the overall framework), when such review should be performed (e.g. only after the third line of defense considered the approach ineffective) and by whom (e.g. only by large and complex firms). Overall many respondents asked for more details to be provided.

33. The EBA notes that firms must ensure that their approach to AML/CFT is effective and in line with applicable legal and regulatory obligations. As part of this, firms should consider whether an independent effectiveness review of their AML/CFT systems and controls is needed and if it is needed, what its scope should be. The review could take place on all or some of its policies, controls and procedures and could be done internally or externally, whereby firms also need to take into account the (national) requirements applicable to them – in some Member States, an external review by a certain profession may be required. In any case, firms should be able to justify their approach to their competent authority.

Investment citizenship schemes

34. Lastly, some respondents called for the EBA to include more guidance on investment citizenship schemes or 'golden visas' in the Guidelines and asked to include a specific reference to OECD publications that firms could use as possible source of information in Guideline 1.30.

35. In relation to the investment citizenship schemes, the EBA takes note of the actions recently taken by the co-legislators,[2] but does not see grounds to amend the Guidelines, as the EBA considers these risks to fall under the broader categories of customer risk, country or geographical risks.

36. With regard to the OECD publications, the EBA strongly supports and promotes that firms use publicly available information and knowhow, including publications by intergovernmental organizations. As OECD highlights on its website, there are substantial similarities between the techniques used to launder the proceeds of crimes and to commit tax crimes.[3] It is key for supervisors and firms to enhance their understanding of tax crimes, which the EBA has also stressed in several products, more in particular the Report on competent authorities' approaches to tackling market integrity risks associated with dividend arbitrage schemes (EBA/REP/2020/15), the action plan on dividend arbitrage trading schemes[4] and the revised Internal Governance Guidelines (as per the recent Consultation Paper, EBA/CP/2020/20). At the same time, in the EBA's view, Guideline 1.30 and 1.31 include a sufficiently comprehensive list of sources of information to identify ML/TF risk factors and the list is of a non-exhaustive nature.

[2] At the same time, the European Commission recently launched infringement procedures against Member States with Investor citizenship schemes, and the European Parliament in its resolution of 10 July 2020, called on Member States to phase out all existing citizenship by investment (CBI) or residency by investment (RBI) schemes as soon as possible.

[3] https://www.oecd.org/ctp/crime/about-tax-and-crime.html.

[4] Action plan on dividend arbitrage trading schemes Cum-ExCum-Cum.pdf (europa.eu).

Guidelines

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

1. Compliance and reporting obligations

Status of these guidelines

1. This document contains Guidelines issued pursuant to Article 16 of Regulation (EU) No 1093/2010[5]. In accordance with Article 16(3) of Regulation (EU) No 1093/2010, competent authorities and financial institutions must make every effort to comply with the Guidelines.

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

Reporting requirements

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

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

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

2. Subject matter, scope and definitions

Subject matter

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

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

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

Scope of application

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

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

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

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

Definitions

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

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

legislation[6].

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

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

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

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

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

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

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

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

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

k) '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.

l) '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.

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

n) '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.

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

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

3. Implementation

Date of application

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

Title I: General Guidelines

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

Guideline 1: Risk assessments: key principles for all firms

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

General considerations

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

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

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

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

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

b) the assessment of ML/TF risk.

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

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

1.5. Firms that are credit institutions and investment firms should also refer to the EBA's internal governance guidelines in this context.[7]

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

Keeping risk assessments up to date

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

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

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

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

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

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

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

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

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

i. In respect of individual risk assessments,

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

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

ii. In respect of business-wide risk assessments,

a. law enforcement alerts and reports;

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

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

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

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

Business-wide risk assessments

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

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

1.13. Firms should:

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

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

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

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

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

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

Proportionality

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

Implementation

1.17. Firms should

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

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

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

Linking the business-wide and individual risk assessments

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

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

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

Individual risk assessments

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

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

Initial Customer Due Diligence

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

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

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

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

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

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

Obtaining a holistic view

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

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

Ongoing customer due diligence

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

Sources of information

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

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

a) the European Commission's supranational risk assessment;

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

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

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

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

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

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

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

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

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

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

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

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

g) information from statistical organisations and academia.

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

Guideline 2: Identifying ML/TF risk factors

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

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

Customer risk factors

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

a) Are there adverse media reports or other relevant sources of information about the customer, for example are there any allegations of criminality or terrorism against the customer or the beneficial owner? If so, are these reliable and credible? Firms should determine the credibility of allegations on the basis of the quality and independence of the source of the data and the persistence of reporting of these allegations, among other considerations. Firms should note that the absence of criminal convictions alone may not be sufficient to dismiss allegations of wrongdoing.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

a) Is the customer or the beneficial owner a person included in the lists of persons, groups and entities involved in terrorist acts and subject to restrictive measures[8],

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

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

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

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

d) Is the customer a non-profit organization

i. whose activities or leadership been publicly known to be associated with extremism or terrorist sympathies? Or

ii. whose transaction behaviour is characterized by bulk transfers of large amounts of funds to jurisdictions associated with higher ML/TF riks and high-risk third countries?

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

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

2.8. In addition to the information sources listed in guidelines 1.30 and 1.31, firms should pay particular attention to the FATF's typologies on TF, which are regularly updated.[9]

Countries and geographical areas

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

Products, services and transactions risk factors

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

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

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

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

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

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

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

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

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

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

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

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

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

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

Delivery channel risk factors

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

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

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

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

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

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

ii. took steps to prevent impersonation or identity fraud.

Firms should apply Guidelines 4.29 to 4.31 in those situations.

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

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

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

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

iii. whether they are based in a jurisdiction associated with higher ML/TF risk. Where a third party is based in a high-risk third country that the CEU Commission has identified as having strategic deficiencies, firms must not rely on that third party. However, to the extent permitted by national legislation, reliance may be possible provided that the intermediary is a branch or majority-owned subsidiary of another firm established in the Union, and the firm is confident that the intermediary fully complies with group-wide policies and procedures in line with Article 45 of Directive (EU) 2015/849.[10]

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

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

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

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

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

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

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

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

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

Guideline 3: Assessing ML/TF risk

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

Taking a holistic view

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

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

Weighting risk factors

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

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

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

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

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

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

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

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

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

Categorising risk

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

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

Guideline 4: CDD measures to be applied by all firms

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

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

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

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

Customer due diligence

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

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

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

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

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

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

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

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

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

g) the firm's risk appetite.

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

Financial inclusion and de-risking

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

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

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

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

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

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

Beneficial owners

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

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

b) Firms should document the information obtained.

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

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

Beneficial ownership registers

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

Control through other means

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

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

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

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

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

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

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

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

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

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

Identifying the customer's senior managing officials

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

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

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

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

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

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

4.22. In those cases, firms should clearly document their reasons for identifying the senior manager, rather than the customer's beneficial owner, and must keep records of their actions[11].

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

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

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

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

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

Evidence of identity

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

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

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

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

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

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

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

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

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

ii. could have been unduly influenced by the customer.

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

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

Non-face to face situations

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

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

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

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

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

Using innovative technological means to verify identity

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

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

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

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

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

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

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

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

a) is registered with relevant national authorities to access and store personal data to EU legal standards in compliance with Regulation (EU) 2016/679 (General Data Protection Regulation (GDPR)[12] and legislation by which the GDPR has been implemented;

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

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

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

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

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

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

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

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

Establishing the nature and purpose of the business relationship

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

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

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

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

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

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

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

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

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

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

Simplified customer due diligence

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

4.44. Where there are indications that the risk may not be low, for example where there are grounds to suspect that ML/TF is being attempted or where the firm has doubts about the veracity of the information obtained, SDD must not be applied.[13] Equally, where specific high-risk scenarios apply and there is an obligation to conduct EDD, SDD must not be applied.

Enhanced customer due diligence

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

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

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

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

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

d) all transactions that are

i. complex;

ii. unusually large;

iii. conducted in an unusual pattern; or

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

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

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

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

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

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

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

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

Politically Exposed Persons

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

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

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

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

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

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

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

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

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

High-risk third countries

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

Correspondent relationships

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

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

Unusual transactions

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

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

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

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

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

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

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

Other high-risk situations

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

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

4.64. EDD measures firms should apply may include:

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

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

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

a. information about family members and close business partners;

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

c. adverse media searches.

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

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

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

c. the destination of funds;

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

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

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

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

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

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

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

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

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

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

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

Other considerations

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

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

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

Monitoring

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

4.70. Monitoring should include:

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

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

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

Transaction monitoring

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

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

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

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

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

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

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

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

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

Keeping CDD information up to date

4.76. Firms must keep CDD information up to date.[14]

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

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

Guideline 5: Record-keeping

[14] Article 14(5) of the AMLD

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

a) CDD information;

b) Their risk assessments; and

c) Transactions.

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

Guideline 6: Training

6.1. Firms must make their staff aware of the provisions they have put in place to comply with their AML/CFT obligations.[15]

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

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

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

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

6.3. Firms should ensure that AML/CFT training is

a) Relevant to the firm and its business;

b) Tailored to staff and their specific roles;

c) Updated regularly; and

d) Effective.

Guideline 7: Reviewing effectiveness

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

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

7.2. Firms should consider whether an independent review of their approach may be warranted or required.[16]

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

Title II: Sector-specific Guidelines

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

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

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

Guideline 8: Sectoral guideline for correspondent relationships

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

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

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

Risk factors

Product, service and transaction risk factors

8.4. The following factors may contribute to increasing risk:

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

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

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

8.5. The following factors may contribute to reducing risk:

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

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

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

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

Customer risk factors

8.6. The following factors may contribute to increasing risk:

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

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

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

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

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

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

g) The respondent´s failure to provide the information requested by the correspondent for CDD and EDD purposes, and information on the payer or the payee that is required under Regulation (EU) 2015/847. For this purpose, the correspondent should consider the quantitative and qualitative criteria set out in the Joint Guidelines JC/GL/2017/16.[17]

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

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

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

Country or geographical risk factors

8.8. The following factors may contribute to increasing risk:

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

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

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

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

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

v. without effective AML/CFT supervision.

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

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

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

8.9. The following factors may contribute to reducing risk:

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

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

Measures

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

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

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

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

b) Establish and document the nature and purpose of the service provided, as well as the responsibilities of each institution. This may include setting out, in writing, the scope of the relationship, which products and services will be supplied, and how and by whom the correspondent banking facility can be used (e.g. if it can be used by other banks through their relationship with the respondent).

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

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

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

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

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

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

Respondents based in non-EEA countries

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

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

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

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

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

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

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

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

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

i. the products and services provided to the respondent,

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

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

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

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

Respondents based in EEA countries

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

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

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

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

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

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

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

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

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

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

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

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

d) Requiring increased monitoring on transfers of funds to ensure detection of missing or incomplete information on the payer and or the payee under Regulation (EU) 2015/847 and in line with the Joint Guidelines JC/GL/2017/16.[18]

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

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

Guideline 9: Sectoral guideline for retail banks

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

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

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

Risk factors

Product, service and transaction risk factors

9.4. The following factors may contribute to increasing risk:

a) the product's features favour anonymity;

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

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

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

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

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

9.5. The following factors may contribute to reducing risk:

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

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

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

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

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

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

b) The product can only be held by certain categories of customers, for example pensioners, parents on behalf of their children, or minors until they reach the age of majority.

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

d) There is no overpayment facility.

Customer risk factors

9.6. The following factors may contribute to increasing risk:

a) The nature of the customer, for example:

i. The customer is a cash-intensive undertaking.

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

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

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

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

vi. The customer is a non-resident. Banks should note that Article 16 of Directive 2014/92/EU creates a right for consumers who are legally resident in the European Union to obtain a basic bank account, although the right to open and use a basic payment account applies only to the extent that banks can comply with their AML/CFT obligations and does not exempt banks from their obligation to identify and assess ML/TF risk, including the risk associated with the customer not being a resident of the Member State in which the bank is based.[19]

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

b) The customer's behaviour, for example:

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

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

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

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

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

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

Country or geographical risk factors

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

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

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

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

9.9. The following factor may contribute to reducing risk:

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

Distribution channel risk factors

9.10. The following factors may contribute to increasing risk:

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

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

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

9.11. The following factor may contribute to reducing risk:

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

Measures

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

Enhanced customer due diligence

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

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

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

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

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

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

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

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

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

d) Increasing the frequency of transaction monitoring.

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

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

Simplified customer due diligence

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

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

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

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

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

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

Pooled accounts

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

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

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

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

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

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

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

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

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

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

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

c) conducting ongoing monitoring of the business relationship.

Customers that offer services related to virtual currencies

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

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

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

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

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

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

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

d) Providing custodian wallet services;

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

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

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

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

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

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

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

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

Guideline 10: Sectoral guideline for electronic money issuers

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

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

Risk factors

Product risk factors

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

a) thresholds;

b) the funding method; and

c) utility and negotiability.

10.4. The following factors may contribute to increasing risk:

a) Thresholds: the product allows

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

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

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

b) Funding method: the product can be

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

ii. funded with payments from unidentified third parties;

iii. funded with other e-money products.

c) Utility and negotiability: the product

i. allows person-to-person transfers;

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

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

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

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

vi. allows high-value cash withdrawals.

10.5. The following factors may contribute to reducing risk:

a) Thresholds: the product

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

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

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

b) Funding: the product

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

c) Utility and negotiability: the product

i. does not allow or strictly limits cash withdrawal;

ii. can be used only domestically;

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

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

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

Customer risk factors

10.6. The following factors may contribute to increasing risk:

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

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

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

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

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

10.7. The following factor may contribute to reducing risk:

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

Distribution channel risk factors

10.8. The following factors may contribute to increasing risk:

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

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

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

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

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

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

Country or geographical risk factors

10.10. The following factors may contribute to increasing risk:

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

Measures

Customer Due Diligence measures

10.11. Firms should apply CDD measures to:

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

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

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

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

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

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

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

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

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

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

Enhanced customer due diligence

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

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

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

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

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

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

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

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

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

Simplified customer due diligence

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

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

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

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

c) verifying identity on the basis of fewer sources;

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

e) using alternative methods to verify identity;

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

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

Guideline 11: Sectoral guideline for money remitters

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

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

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

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

Risk factors

Product, service and transaction risk factors

11.5. The following factors may contribute to increasing risk:

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

b) the product or service has a global reach;

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

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

11.6. The following factor may contribute to reducing risk:

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

Customer risk factors

11.7. The following factors may contribute to increasing risk:

a) The customer's business activity:

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

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

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

b) The customer's behaviour:

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

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

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

iv. The customer's transactions are always just below applicable thresholds, including the CDD threshold for occasional transactions in Article 11(b) of Directive (EU) 2015/849 and the EUR 1 000 threshold specified in Article 5(2) of Regulation (EU) 2015/847.[20] Firms should note that the threshold in Article 5(2) of Regulation (EU) 2015/847 applies only to transactions that are not funded by cash or anonymous electronic money.

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

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

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

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

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

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

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

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

11.8. The following factors may contribute to reducing risk:

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

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

Distribution channel risk factors

11.9. The following factors may contribute to increasing risk:

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

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

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

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

i. represent more than one principal;

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

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

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

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

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

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

11.10. The following factors may contribute to reducing risk:

a) Agents are themselves regulated financial institutions.

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

Country or geographical risk factors

11.11. The following factors may contribute to increasing risk:

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

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

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

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

Measures

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

11.13. Firms should in any case put in place:

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

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

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

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

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

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

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

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

Use of agents

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

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

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

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

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

Guideline 12: Sectoral guideline for wealth management

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

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

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

Risk factors

Product, service and transaction risk factors

12.4. The following factors may contribute to increasing risk:

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

b) very high-value transactions;

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

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

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

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

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

Customer risk factors

12.5. The following factors may contribute to increasing risk:

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

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

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

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

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

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

Country or geographical risk factors

12.6. The following factors may contribute to increasing risk:

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

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

Measures

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

Enhanced customer due diligence

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

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

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

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

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

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

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

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

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

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

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

c) Establishing the destination of funds.

Guideline 13: Sectoral guideline for trade finance providers

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

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

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

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

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

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

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

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

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

Risk factors

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

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

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

Transaction risk factors

13.10. The following factors may contribute to increasing risk:

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

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

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

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

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

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

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

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

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

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

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

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

13.11. The following factors may contribute to reducing risk:

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

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

Customer risk factors

13.12. The following factors may contribute to increasing risk:

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

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

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

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

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

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

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

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

13.13. The following factors may contribute to reducing risk:

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

Country or geographical risk factors

13.14. The following factors may contribute to increasing risk:

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

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

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

13.15. The following factors may contribute to reducing risk:

a) The trade is within the EU/EEA.

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

Measures

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

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

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

Enhanced customer due diligence

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

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

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

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

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

13.22. Checks on transactions may include:

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

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

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

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

Simplified customer due diligence

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

Guideline 14: Sectoral guideline for life insurance undertakings

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

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

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

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

14.5. Intermediaries may also find these guidelines useful.

Risk factors

Product, service and transaction risk factors

14.6. The following factors may contribute to increasing risk:

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

i. payments from unidentified third parties;

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

iii. cash payments.

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

c) Negotiability, for example the product can be:

i. traded on a secondary market;

ii. used as collateral for a loan.

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

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

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

b) has no surrender value;

c) has no investment element;

d) has no third party payment facility;

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

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

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

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

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

j) cannot be used as collateral;

k) does not allow cash payments;

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

Customer and beneficiary risk factors

14.8. The following factors may contribute to increasing risk:

a) The nature of the customer, for example:

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

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

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

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

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

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

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

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

b) The customer's behaviour:

i. In relation to the contract, for example:

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

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

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

d. the customer incurs a high cost by seeking early termination of a product;

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

f. the customer's request to change or increase the sum insured and/or the premium payment are unusual or excessive.

ii. In relation to the beneficiary, for example:

a. the insurer is made aware of a change in beneficiary only when the claim is made;

b. the customer changes the beneficiary clause and nominates an apparently unrelated third party;

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

iii. In relation to payments, for example:

a. the customer uses unusual payment methods, such as cash or structured monetary instruments or other forms of payment vehicles fostering anonymity;

b. payments from different bank accounts without explanation;

c. payments from banks that are not established in the customer's country of residence;

d. the customer makes frequent or high-value overpayments where this was not expected;

e. payments received from unrelated third parties;

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

14.9. The following factors may contribute to reducing risk. In the case of corporate-owned life insurance, the customer is:

a) a credit or financial institution that is subject to requirements to combat money laundering and the financing of terrorism and supervised for compliance with these requirements in a manner that is consistent with Directive (EU) 2015/849;

b) a public administration or a public enterprise from an EEA jurisdiction.

Distribution channel risk factors

14.10. The following factors may contribute to increasing risk:

a) non-face-to-face sales, such as online, postal or telephone sales, without adequate safeguards, such as electronic signatures or electronic identification means that comply with Regulation (EU) No 910/2014;

b) long chains of intermediaries;

c) an intermediary is used in unusual circumstances (e.g. unexplained geographical distance).

14.11. The following factors may contribute to reducing risk:

a) Intermediaries are well known to the insurer, who is satisfied that the intermediary applies CDD measures commensurate to the risk associated with the relationship and in line with those required under Directive (EU) 2015/849.

b) The product is only available to employees of certain companies that have a contract with the insurer to provide life insurance for their employees, for example as part of a benefits package.

Country or geographical risk factors

14.12. The following factors may contribute to increasing risk:

a) The insurer, the customer, the beneficial owner, the beneficiary or the beneficial owner of the beneficiary are based in, or associated with, jurisdictions associated with higher ML/TF risk. Firms should pay particular attention to jurisdictions without effective AML/CFT supervision.

b) Premiums are paid through accounts held with financial institutions established in jurisdictions associated with higher ML/TF risk. Firms should pay particular attention to jurisdictions without effective AML/CFT supervision.

c) The intermediary is based in, or associated with, jurisdictions associated with higher ML/TF risk. Firms should pay particular attention to jurisdictions without effective AML/CFT supervision.

14.13. The following factors may contribute to reducing risk:

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

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

Measures

14.14. Article 13(5) of Directive (EU) 2015/849 provides that, for life insurance business, firms must apply CDD measures not only to the customer and beneficial owner but also to the beneficiaries as soon as they are identified or designated. This means that firms must:

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

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

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

14.16. Where the firm knows that the life insurance has been assigned to a third party, who will receive the value of the policy, they must identify the beneficial owner at the time of the assignment.

14.17. In order to comply with Article 13(6) of Directive (EU) 2015/849, when the beneficiaries of trusts or of similar legal arrangements are a class of persons or designated by certain characteristics, firms should obtain sufficient information to be satisfied that the identities of the beneficiaries can be established at the time of payout or at the time of the exercise by the beneficiaries of their vested rights.

Enhanced customer due diligence

14.18. To comply with Article 18a in respect of relationships or transactions involving high-risk third countries, firms should apply the EDD measures set out in this regard in Title I. The following EDD measures may be appropriate in all other high-risk situation:

a) Where the customer makes use of the 'free look'/'cooling-off' period, the premium should be refunded to the customer's bank account from which the funds were paid. Firms should ensure that they have verified the customer's identity in line with Article 13 of Directive (EU) 2015/849 before making a refund, in particular where the premium is large or the circumstances appear otherwise unusual. Firms should also consider whether the cancellation gives rise to suspicion about the transaction and whether submitting a suspicious activity report would be appropriate.

b) Additional steps may be taken to strengthen the firm's knowledge about the customer, the beneficial owner, the beneficiary or the beneficiary's beneficial owner, the third party payers and payees. Examples include:

i. not using the derogation in Article 14(2) of Directive (EU) 2015/849, which provides for an exemption from upfront CDD;

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

iii. obtaining additional information to establish the intended nature of the business relationship;

iv. obtaining additional information on the customer and updating more regularly the identification data of the customer and beneficial owner;

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

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

vii. establishing the customer's source of wealth and source of funds, for example employment and salary details, inheritance or divorce settlements;

viii. where possible, identifying the beneficiary and verifying their identity at the beginning of the business relationship, rather than waiting until they are identified or designated, bearing in mind that the beneficiary can change over the term of the policy;

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

x. in line with Articles 20 and 21 of Directive (EU) 2015/849, taking measures to determine whether the customer is a PEP and taking reasonable measures to determine whether the beneficiary or the beneficiary's beneficial owner is a PEP at the time of assignment, in whole or in part, of the policy or, at the latest, at the time of payout;

xi. requiring the first payment to be carried out through an account in the customer's name with a bank subject to CDD standards that are not less robust than those required under Directive (EU) 2015/849.

14.19. Article 20 of Directive (EU) 2015/849 requires that, where the risk associated with a PEP relationship is high, firms must not only apply CDD measures in line with Article 13 of the Directive but also inform senior management before the payout of the policy so that senior management can take an informed view of the ML/TF risk associated with the situation and

decide on the most appropriate measures to mitigate that risk; in addition, firms must conduct EDD on the entire business relationship.

14.20. Firms should:

a) obtain additional information on the business relationship so as to be able to understand the nature of the relationship between the customer/the insured and the beneficiary, and of the relationship between the payer and the beneficiary if the payer is different from the customer/the insured; and

b) enhance their scrutiny on the source of funds.

14.21. Where the beneficiary is a PEP and is expressly named, firms should not wait until the payout of the policy to conduct the enhanced scrutiny of the entire business relationship.

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

Simplified customer due diligence

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

a) Firms may be able to assume that the verification of the identity of the customer is fulfilled on the basis of a payment drawn on an account that the firm is satisfied is in the sole or joint name of the customer with an EEA-regulated credit institution.

b) Firms may be able to assume that the verification of the identity of the beneficiary of the contract is fulfilled on the basis of a payment made to an account in the beneficiary's name at a regulated EEA credit institution.

Guideline 15: Sectoral guideline for investment firms

15.1. Investment firms as defined in point (1) of Article 4(1) of Directive 2014/65/EUshould consider when providing or executing investment services or activities as defined in point (2) of Article 4(1) of Directive (EU) 2014/65 the following risk factors and measures alongside those set out in Title I of these guidelines. The sectoral guideline 12 may also be relevant in this context.

15.2. To comply with their obligations under Directive (EU) 2015/849, firms in this sector should consider that:

a) ML/TF risk in this sector is driven primarily by the risk associated with the clients whom investment firms serve; and

b) the nature of the activities which investment firms undertake means that they may be exposed to predicate offences such as market abuse, which may lead to ML/TF.

Risk factors

Product, service or transaction risk factors

15.3. The following factors may contribute to increasing risk:

a) transactions are unusually large, in the context of the customer's profile;

b) settlement arrangements that are non-standard or appear irregular;

c) mirror trades or transactions involving securities used for currency conversion that appear unusual or have no apparent business or economic purposes;

d) the product or service is structured in a way that may present difficulties in identifying the customers; third party payments are possible.

15.4. The following factors may contribute to reducing risk:

a) The product or service is subject to mandatory transparency and/or disclosure requirements.

Customer risk factors

15.5. The following factors may contribute to increasing risk:

a) The customer's behaviour, for example:

i. the rationale for the investment lacks an obvious economic purpose;

ii. the customer asks to repurchase or redeem a long-term investment within a short period after the initial investment or before the payout date without a clear rationale, in particular where this results in financial loss or payment of high transaction fees;

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

iv. unwillingness to provide CDD information on the customer and the beneficial owner;

v. frequent changes to CDD information or payment details;

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

vii. the circumstances in which the customer makes use of the 'cooling-off' period give rise to suspicion;

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

ix. the customer wishes to structure the relationship in such a way that multiple parties, for example nominee companies, are used in different jurisdictions, particularly where these jurisdictions are associated with higher ML/TF risk.

b) The customer's nature, for example:

i. the customer is a company, a trust or other legal arrangements having a structure or functions similar to trusts, established in a jurisdiction associated with higher ML/TF risk (firms should pay particular attention to those jurisdictions that do not comply effectively with international tax and information sharing transparency standards);

ii. the customer is an investment vehicle that carries out little or no due diligence on its own clients;

iii. the customer is an unregulated third party investment vehicle;

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

v. the customer or the beneficial owner is a PEP or holds another prominent position that might enable them to abuse their position for private gain;

vi. the customer is a non-regulated nominee company with unknown shareholders.

c) The customer's business, for example the customer's funds are derived from business in sectors that are associated with a higher risk of financial crime, such as construction, pharmaceuticals and healthcare, the arms trade and defence, the extractive industries or public procurement.

15.6. The following factors may contribute to reducing risk:

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

b) The customer is a government body from an EEA jurisdiction.

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

Distribution channel risk factors

15.7. The following factors may contribute to increasing the risk:

a) Complexity in the chain of reception and transmission of orders;

b) Complexity in the distribution chain of investment products;

c) The trading venue has members or participants located in high-risk jurisdictions

Country or geographical risk factors

15.8. The following factors may contribute to increasing risk:

a) The investor or their custodian is based in a jurisdiction associated with higher ML/TF risk.

b) The funds come from a jurisdiction associated with higher ML/TF risk.

Measures

15.9. When developing their AML/CFT policies and procedures to comply with their obligations under Directive (EU) 2015/849, firms in this sector should consider that depending on the type of activity they perform, they will be subject to rules under which they have to gather extensive information about their customers. Where this is the case, they should consider the extent to which information obtained for MiFID II and EMIR compliance purposes can be used also to meet their CDD obligations in standard situations.

15.10. In particular, investment managers typically need to develop a good understanding of their customers to help them identify suitable investment portfolios. The information gathered will be similar to that which firms obtain for AML/CFT purposes.

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

a) identify and, where necessary, verify the identity of the underlying investors of the firm's customer where the customer is an unregulated third party investment vehicle;

b) understand the reason for any payment or transfer to or from an unverified third party.

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

Guideline 16: Sectoral guideline for providers of investment funds

16.1. The provision of investment funds can involve multiple parties, such as the fund manager, appointed advisers, the depositary and sub-custodians, registrars and, in some cases, prime brokers. Similarly, the distribution of these funds can involve parties such as tied agents, advisory and discretionary wealth managers, platform service providers and independent financial advisers.

16.2. The type and number of parties involved in the fund's distribution process depends on the nature of the fund and may affect how much the fund knows about its customer and investors. The fund or, where the fund is not itself an obliged entity, the fund manager will retain responsibility for compliance with AML/CFT obligations, although aspects of the fund's CDD obligations may be carried out by one or more of these other parties subject to certain conditions.

16.3. Investment funds may be used by persons or entities for ML/TF purposes:

a) Retail funds are often distributed on a non-face-to-face basis; access to such funds is often easy and relatively quick to achieve, and holdings in such funds can be transferred between different parties.

b) Alterative investment funds, such as hedge funds, real estate and private equity funds, tend to have a smaller number of investors, which can be private individuals as well as institutional investors (pension funds, funds of funds). Such funds that are designed for a limited number of high-net-worth individuals, or for family offices, can have an inherently higher risk of abuse for ML/TF purposes than retail funds, since investors are more likely to be in a position to exercise control over the fund assets. If investors exercise control over the assets, such funds are personal asset-holding vehicles, which are mentioned as a factor indicating potentially higher risk in Annex III to Directive (EU) 2015/849.

c) Notwithstanding the often medium- to long-term nature of the investment, which can contribute to limiting the attractiveness of these products for money laundering purposes, they may still appeal to money launderers on the basis of their ability to generate growth and income.

16.4. This sectoral guideline is directed at:

a) investment funds marketing their own shares or units, under Article 3(2)(d) of Directive (EU) 2015/849; and

b) funds managers, where an investment fund is not incorporated.

Other parties involved in the provision or distribution of the fund, for example intermediaries, may have to comply with their own CDD obligations and should refer to relevant chapters in these guidelines as appropriate.

For funds and fund managers, the sectoral guidelines 8, 14 and 15 may also be relevant.

Risk factors

Product, service or transaction risk factors

16.5. The following factors may contribute to increasing the risk associated with the fund:

a) The fund is designed for a limited number of individuals or family offices, for example a private fund or single investor fund.

b) It is possible to subscribe to the fund and then quickly redeem the investment without the investor incurring significant administrative costs;

c) Units of or shares in the fund can be treated without the fund or fund manager being notified at the time of the trade;

d) Information about the investor is divided among several subjects.

16.6. The following factors may contribute to increasing the risk associated with the subscription:

a) The subscription involves accounts or third parties in multiple jurisdictions, in particular where these jurisdictions are associated with a high ML/TF risk as defined in guideline 2.9 to 2.15 of Title I.

b) The subscription involves third party subscribers or payees, in particular where this is unexpected.

16.7. The following factors may contribute to reducing the risk associated with the fund:

a) Payments to and from third parties are not allowed.

b) The fund is open to small-scale investors only, with investments capped.

Customer risk factors

16.8. The following factors may contribute to increasing risk. The customer's behaviour is unusual, for example:

a) The rationale for the investment lacks an obvious strategy or economic purpose or the customer makes investments that are inconsistent with the customer's overall financial situation, where this is known to the fund or fund manager.

b) The customer requests the repeated purchase and/or sale of units or shares within a short period of time after the initial investment or before the payout date without a clear strategy or rationale, in particular where this results in financial loss or payment of high transaction fees.

c) The customer transfers funds in excess of those required for the investment and asks for surplus amounts to be reimbursed.

d) The customer uses multiple accounts without previous notification, especially when these accounts are held in multiple jurisdictions or jurisdictions associated with higher ML/TF risk.

e) The customer wishes to structure the relationship in such a way that multiple parties, for example non-regulated nominee companies, are used in different jurisdictions, particularly where these jurisdictions are associated with higher ML/TF risk.

f) The customer suddenly changes the settlement location without rationale, for example by changing the customer's country of residence.

16.9. The following factors may contribute to reducing risk:

a) the customer is an institutional investor whose status has been verified by an EEA government agency, for example a government-approved pensions scheme;

b) the customer is a firm subject to AML/CFT requirements that are not less robust than those required by Directive (EU) 2015/849.

Distribution channel risk factors

16.10. The following factors may contribute to increasing risk:

a) Complex distribution channels that limit the fund's oversight of its business relationships and restrict its ability to monitor transactions, for example the fund uses a large number of sub-distributors for distribution in third countries;

b) the distributor is located in a jurisdiction associated with higher ML/TF risk as defined in the general part of these guidelines.

16.11. The following factors may indicate lower risk:

a) The fund admits only a designated type of low-risk investor, such as regulated firms investing as a principal (e.g. life companies) or corporate pension schemes.

b) The fund can be purchased and redeemed only through a firm subject to AML/CFT requirements that are not less robust than those required by Directive (EU) 2015/849.

Country or geographical risk factors

16.12. The following factors may contribute to increasing risk:

a) The customers' or beneficial owners' funds have been generated in jurisdictions associated with higher ML/TF risk, in particular those associated with higher levels of predicate offences to money laundering.

b) The customer requests their investment to be redeemed to an account in a credit institution located in a jurisdiction associated with higher ML/TF risk.

Measures

16.13. The measures funds or fund managers should take to comply with their CDD obligations will depend on how the customer or the investor (where the investor is not the customer) comes to the fund. The fund or fund manager should also take risk-sensitive measures to identify and verify the identity of the natural persons, if any, who ultimately own or control the customer (or on whose behalf the transaction is being conducted), for example by asking the prospective customer to declare, when they first apply to join the fund, whether they are investing on their own behalf or whether they are an intermediary investing on someone else's behalf.

16.14. The customer is:

a) a natural or legal person who directly purchases units of or shares in a fund on their own account, and not on behalf of other, underlying investors; or

b) a firm that, as part of its economic activity, directly purchases units of or shares in its own name and exercises control over the investment for the ultimate benefit of one or more third parties who do not control the investment or investment decisions; or

c) a firm, for example a financial intermediary, that acts in its own name and is registered in the fund's share/units register but acts on the account of, and pursuant to specific instructions from, one or more third parties (e.g. because the financial intermediary is a nominee, broker, multi-client pooled account/omnibus type account operator or operator of a similar passive-type arrangement); or

d) a firm's customer, for example a financial intermediary's customer, where the firm is not registered in the fund's share/units register (e.g. because the

investment fund uses a financial intermediary to distribute fund shares or units, and the investor purchases units or shares through the firm and is registered in the fund's share/units register).

Enhanced Customer Due Diligence

16.15. In the situations described in guidelines 16.14 (a) and (b), examples of EDD measures a fund or fund manager should apply in high-risk situations include:

a) obtaining additional customer information, such as the customer's reputation and background, before the establishment of the business relationship;

b) taking additional steps to further verify the documents, data or information obtained;

c) obtaining information on the source of funds and/or the source wealth of the customer and of the customer's beneficial owner;

d) requiring that the redemption payment is made through the initial account used for investment or an account in the sole or joint name of the customer;

e) increasing the frequency and intensity of transaction monitoring;

f) requireng that the first payment is made through a payment account held in the sole or joint name of the customer with an EEA-regulated credit or financial institution or a regulated credit or financial institution in a third country that has AML/CFT requirements that are not less robust than those required by Directive (EU) 2015/849;

g) obtaining approval from senior management at the time the first transaction;

h) enhanced monitoring of the customer relationship and individual transactions.

16.16. In the situations described in guideline 16.14 (c), where the risk is increased, in particular where the fund is designated for a limited number of investors, EDD measures must apply and may include those set out in guideline 16.15 above.

16.17. Where a financial intermediary is based in a third country and has established a relationship similar to correspondent banking with the fund or the fund's manager, the measures described in guidelines 16.20 and 16.21 are not applicable. In such cases, to discharge their obligations under Article 19 of the Directive (EU) 2015/849, firms should apply toward the intermediary the enhanced due diligence measures listed in Sectoral Guideline 8. 14 to 8.17.

16.18. In the situations described in guideline 16.14(d) where the risk is increased, in particular where the fund is designated for a limited number of investors, EDD measures must apply and may include those set out in guideline 16.15 above.

Simplified Customer Due Diligence

16.19. In the situations described in guidelines 16.14 (a) and 16.14 (b), in lower risk situations, to the extent permitted by national legislation, and provided that the funds are verifiably being transferred to or from a payment account held in the customer's sole or joint name with an EEA-regulated credit or financial institution, an example of the SDD measures the fund or fund manager may apply is using the source of funds to meet some of the CDD requirements.

16.20. In the situations described in guideline 16.14(c) , where the financial intermediary is the fund or fund manager's customer, the fund or fund manager should apply risk-sensitive CDD measures to the financial intermediary. The fund or fund manager should also take risk-sensitive measures to identify, and verify the identity of, the investors underlying the financial intermediary, as these investors could be beneficial owners of the funds invested through the intermediary. To the extent permitted by national law, in low-risk situations, funds or fund managers may apply SDD measures similar to those described in Title I of these guidelines, subject to the following conditions:

a) The financial intermediary is subject to AML/CFT obligations in an EEA jurisdiction or in a third country that has AML/CFT requirements that are not less robust than those required by Directive (EU) 2015/849.

b) The financial intermediary is effectively supervised for compliance with these requirements.

c) The fund or fund manager has taken risk-sensitive steps to be satisfied that the ML/TF risk associated with the business relationship is low, based on, *inter alia*, the fund or fund manager's assessment of the financial intermediary's business, the types of clients the intermediary's business serves and the jurisdictions the intermediary's business is exposed to.

d) The fund or fund manager has taken risk-sensitive steps to be satisfied that the intermediary applies robust and risk-sensitive CDD measures to its own customers and its customers' beneficial owners. As part of this, the fund or fund manager should take risk-sensitive measures to assess the adequacy of the intermediary's CDD policies and procedures, for example by referring to publicly available information about the intermediary's compliance record or liaising directly with the intermediary.

e) The fund or fund manager has taken risk-sensitive steps to be satisfied that the intermediary will provide CDD information and documents on the underlying investors immediately upon request, for example by including relevant provisions in a contract with the intermediary or by sample-testing the intermediary's ability to provide CDD information upon request.

16.21. In the situations described in guideline 16.14 (d), the fund or fund manager should apply risk-sensitive CDD measures to the ultimate investor as the fund or fund manager's customer. To meet its CDD obligations, the fund or fund manager may rely upon the intermediary in line with, and subject to, the conditions set out in Chapter II, Section 4, of Directive (EU) 2015/849.

16.22. To the extent permitted by national law, in low-risk situations, funds or fund managers may apply SDD measures. Provided that the conditions listed in guideline 16.20 are met, SDD measures may consist of the fund or fund manager obtaining identification data from the fund's share register, together with the information specified in Article 27(1) of Directive (EU) 2015/849, which the fund or fund manager must obtain from the intermediary within a reasonable timeframe. The fund or fund manager should set that timeframe in line with the risk-based approach.

Guideline 17 Sectoral guideline for regulated crowdfunding platforms

17.1. For the purposes of this sectoral Guideline, the following definitions set out in Article 2(1) of Regulation (EU) 2020/1503 are used and should apply: 'crowdfunding service', 'crowdfunding platform', 'crowdfunding service provider' (CSP), 'project owner' and 'investor'. This sectoral Guideline refers to 'customers' in the meaning of 'clients', as defined in Article 2(1) (g) of that same regulation.

17.2. CSPs should recognise the risks arising from the borderless nature of crowdfunding platforms where the CSP's customers can be located anywhere in the world, including high-risk jurisdictions. CSPs should know their customers to prevent their crowdfunding platforms from being used to fund fictitious investment projects with illicit funds or being misused for TF purposes where a fictitious reason is given for a crowdfunding project, which never materialises and the funds obtained from crowdfunding are then used to finance a terror attack.

17.3. CSPs should consider the risk factors and measures set out in this sectoral guideline in addition to those set out in Title I. CSPs that provide investment services should also refer to the sectoral guidance 16.

Risk factors

Product, service and transaction risk factors

17.4. CSP should take into account the following risk factors as potentially contributing to increased risk:

a) The CSP collects funds through the crowdfunding platform but allows for later onward transmission, including business models where:

   i. money is collected for an undetermined project and consequently held in the investor's account until the project is determined; or

   ii. money is collected but may be returned to the investors where the fundraising target is not met, or where the project owner has not received the money.

b) The CSP permits early redemption of investments, early repayment of loans, or resale of the investments or loans through secondary markets.

c) The CSP places no restriction on the size, volume or value of the transactions, loading or redemption processed through the crowdfunding platform, or the amount of funds to be stored in individual investor accounts.

d) The CSP allows investors to make a payment to the project owner through the crowdfunding platform with instruments, which are either outside the scope of any regulatory regime, or are subject to less robust AML/CFT requirements than those required by Directive (EU) 2015/849.

e) The CSP accepts cash investments from or permits cash withdrawals by investors that are individuals or unregulated legal entities through the crowdfunding platform.

f) The CSP provides for investors or lenders financial leverage or privileged redemption or guaranteed return.

g) The CSP does not confirm its commitment to buy back securities and there is no time for such buy-back.

h) For non-equity instruments, the nominal interest rate, the date from which interest becomes payable, the due dates for interest payments, the maturity date and the applicable yield are not understandably provided.

i) The CSP allows payments through the crowdfunding platform in virtual currencies.

j) The CSP allows investors and project owners to maintain multiple accounts on the crowdfunding platform where they are not linked to specific crowdfunding projects.

k) The CSP allows transfers between investors or project owners on the crowdfunding platform.

17.5. The CSP should take into account the following risk factors as potentially contributing to reduced risk:

a) The CSP requires that funds for investment, redemption, lending, or repayment are verifiably drawn from, or sent to, an account held in the customer's sole or joint name at a credit institution or financial institution, or a payment institution authorised under Directive (EU) 2015/2366, subject to AML/CFT requirements not less robust than those required by Directive (EU) 2015/849.

b) The CSP sets low-value limits on investment, lending, redemption, and repayment processed through the crowdfunding platform, in terms of monetary size and number of payments.

c) The CSP requires a fixed or longer holding period for investments, or repayment period for loans acquired through the crowdfunding platform.

d) The CSP limits the amount of funds that can be stored in any account at any one time on the crowdfunding platform.

e) The CSP utilises technology to spot whether the investors or project owners use VPN or other technologies that hide the real location and device when using the crowdfunding platform.

f) The CSP does not allow the creation of multiple accounts on the crowdfunding platform.

Customer risk factors

17.6. The CPS should take into account the following risk factors as potentially contributing to increased risk:

a) The customer's nature or behaviour is unusual, for example:

i. The rationale for the investment or loan lacks an obvious strategy or economic purpose.

ii. The investor asks to redeem an investment within a short period after the initial investment.

iii. The investor asks for privileged conditions or for fixed return on investment.

iv. The investor or the project owner transfers funds to the platform in excess of those required for the project/loan, and then asks for surplus amounts to be reimbursed;

v. The investor or the project owner is an individual or a legal person associated with higher levels of ML risks;

vi. The project owner accelerates, unexpectedly or without reasonable explanation, an agreed redemption/repayment schedule, by means either or lump sum payments or early termination; or

vii. The project owner appears to be reluctant in providing information about the project or initiative seeking crowdfunding.

viii. The source of the funds for the investment is unclear and the investor is reluctant to provide this information when requested by the CSP. The degree of invested assets exceeds the volume of the investor's estimated liquid assets. The funds invested are borrowed.

ix. Investor is not residing at or does not have any other connections with the country of the crowdfunding platform or the object of the investment.

x. Investor or project owner is a PEP.

xi. Investor is refusing to provide the required CDD.

b) The investor or the project owner transfer virtual currency.

c) The investor or the project owner were involved in negative news.

d) The investor or the project owner are under sanctions.

Distribution channel risk factors

17.7. The CSP should take into account the following risk factors as potentially contributing to increased risk

a) The CSP operates the crowdfunding platform entirely online without adequate safeguards, such as electronic identification of a person using electronic signatures or electronic identification means that comply with Regulation (EU) No 910/2014.

b) Customers are on-boarded non-face-to-face through the crowdfunding platform without any safeguards in place.

c) The CSP is operating outside any regulatory regime, and therefore the measures which would otherwise be in place to detect and mitigate potential use of the crowdfunding platform for ML/TF purposes may not be in place. This is without prejudice to the application of Guideline 11.

17.8. The CSP should take into account the following risk factors as potentially contributing to decreased risk:

a) The CSP uses a credit institution or financial institution to perform money handling or remittance services. Alternatively, the CSP opens an account in its own name in a regulated credit institution or financial institution, through which money transactions flow between project owners and investors.

b) The CSP operating the crowdfunding platform is authorised as a payment institution under Directive (EU) 2015/2366 or acts as an agent of a payment institution authorised under Directive (EU) 2015/2366 and directly processes money transactions among investors and project owners. This is without prejudice to the application of Guideline 11.

c) Investors and project owners have been met face-to-face or have been introduced by a regulated financial intermediary (credit institution or investment firm) who has carried out a full CDD on all the customers (project owners and investors)

Country or geographical risk factors

17.9. The CSP should take into account the following risk factors as potentially contributing to increased risk:

a) The CSP has a global reach, matching investors, project owners and projects from different jurisdictions.

b) The funds are derived from personal or business links to a jurisdiction identified by credible sources as having significant levels of corruption or other criminal activities, such as terrorism, money laundering, production and supply of illicit drugs, or other predicate offences.

c) The project owner or the investor, or their respective beneficial owners, where relevant, are located in a jurisdiction associated with higher ML/TF risks, or one without effective AML/CFT supervision. CSPs should pay particular attention to jurisdictions known to provide funding or support for terrorist activities or where groups committing terrorist offences are known to be operating, and jurisdictions subject to financial sanctions, embargoes or measures (issued, for example, by the EU or the United Nations) related to terrorism, financing of terrorism, or proliferation.

Measures

17.10. CSPs that are obliged entities as payment institutions authorised under Directive (EU) 2015/2366 or act as an agent of a payment institution authorised under Directive (EU) 2015/2366 should apply relevant measures in sectoral guideline 11 also to their crowdfunding services.

17.11. CSPs that are obliged entities as investment firms authorised under Directive (EU) 2014/65 should apply relevant measures in sectoral guideline 15 also to their crowdfunding services.

17.12. CSPs that are obliged entities as credit institutions authorized under Directive (EU) 2013/36 should apply relevant measures in sectoral guideline 9 also to their crowdfunding services.

17.13. An undertaking authorised as a CSP under national law and that is subject to national AML/CFT law should apply this sectoral guideline and other relevant sectoral guidelines *mutatis mutandis* in order to ensure harmonised and effective AML/CFT supervision of CSPs established in the Union.

Customer due diligence

17.14. CSPs should apply CDD measures in line with Title I to all their customers, be them investors or project owners.

17.15. CSPs that rely on credit institutions or financial institutions to collect funds from or transfer funds to customer, should refer to the distribution channel risk factors in Title I and in particular, satisfy themselves that these credit institutions or financial institutions have put in place appropriate customer due diligence measures.

Enhanced customer due diligence

17.16. Where the risk associated with an occasional transaction or a business relationship is increased CSPs platform should apply the following EDD measures:

a) obtaining additional information from the customers transacting on the platform, such as their investment intention and experience, background and reputation, before the establishment of the business relationship (for example, by carrying out open source or adverse media searches or commissioning a third party intelligence report to build a more complete customer profile);

b) taking additional steps to further verify the documents, data, or information obtained;

c) obtaining information on the source of funds of the customers and their beneficial owners;

d) requiring that the redemption payment or loan repayment is made through the initial account used for investment or an account in the sole or joint name of the customers concerned;

e) increasing the frequency and intensity of transaction monitoring;

f) requiring that the first payment of the investment or loan to be made through a payment account held in the sole or joint name of the party concerned with an EEA-regulated credit or financial institution or a regulated credit or financial

institution in a third country that has AML/CFT requirements not less robust than those required by Directive (EU) 2015/849;

g) obtaining approval from senior management at the time of the transaction when a customers uses the platform for the first time;

h) enhanced monitoring of the customer relationship and individual transactions.

Simplified customer due diligence

17.17. In low-risk situations, and to the extent permitted by national legislation, crowdfunding platforms may apply SDD measures, which may include:

a) verifying the customer's and, where applicable, the beneficial owner's identities during the establishment of the business relationship, in accordance with Article 14(2) of Directive (EU) 2015/849; or

b) assuming that a payment drawn on an account in the sole or joint name of the customer at a regulated credit or financial institution in an EEA country satisfies the requirements stipulated by Article 13(1)(a) and (b) of Directive (EU) 2015/849.

Guideline 18: Sectoral guideline for payment initiation service providers (PISPs) and account information service providers (AISPs)

18.1. When applying this Guideline, firms should have regard to the definitions in point 18 and 19 of Article 4 of Directive (EU) 2015/2366 in accordance with which:

a) a payment initiation service provider (PISP) is a payment service provider pursuing payment initiation services which in accordance with the definition in point 15 of Article 4 of Directive (EU) 2015/2366 means services to initiate a payment order at the request of the payment service user with respect to a payment account held at another payment service provider);

b) an account information service provider (AISP) is a payment service provider offering account information services which in accordance with the definition in point 16 of Article 4 of Directive (EU) 2015/2366 means online services to provide consolidated information on one or more payment accounts held by the payment service user with either another payment service provider or with more than one payment service provider).

18.2. Firms should take into account that despite PISPs and AISPs being obliged entities under Directive (EU) 2015/849, the inherent ML/TF risk associated with them is limited due to the fact that :

a) PISPs, although being involved in the payment chain, do not execute themselves the payment transactions and do not hold payment service users' (PSUs') funds;

b) AISPs are not involved in the payment chain and do not hold payment service user's funds.

18.3. When offering payment initiation services or account information services, PISPs and AISPs should take into account, together with Title I, the provision set out in this sectoral guideline.

Risk factors

Customer risk factors

18.4. When assessing ML/TF risks, PISPs and AISPs should take into account at least the following factors as potentially contributing to increased risk:

a) For PISPs: The customer transfers funds from different payment accounts to the same payee that, together, amount to a large sum without a clear economic or legitimate rationale, or that give the PISP reasonable grounds to suspect that the customer is trying to evade specific monitoring thresholds;

b) For AISPs: the customer transfers funds from different payment accounts to the same

payee, or receives funds on different payments accounts from the same payer, that, together, amount to a large sum without a clear economic or legitimate rationale, or that gives the AISP reasonable grounds to suspect that the customer is trying to evade specific monitoring thresholds.

Distribution channel risk factors

18.5. When assessing ML/TF risks, PISPs and AISPs may wish to refer to the ESAs' Opinion on the use of innovative solution in the customer due diligence process (JC 2017 81).

Country or geographical risk factor

18.6. When assessing ML/TF risks, PISPs and AISPs should at least take into account the following factors as potentially contributing to increased risk in particular if the customer uses multiple accounts held with different ASPSPs to make payments:

a) For PISPs: the customer initiates a payment to a jurisdiction associated with higher ML/TF risk or a high-risk third country or someone with known links to those jurisdictions.

b) For AISPs: The customer receives funds from, or sends funds to, jurisdictions associated with higher ML/TF risk or a high-risk third country or from/to someone with known links to those jurisdictions, or the customer connects payment accounts held in the name of multiple persons in more than one jurisdiction..

18.7. When assessing ML/TF risks, AISPs and PISPs should take into account the following factors as potentially contributing to decreased risk:

a) For PISPs: the customer initiates a payment transaction to an EEA member country or to third country that has AML/CFT requirements that are not less robust than those required by Directive (EU) 2015/849.

b) For AISPs: the customer's payment accounts are held in an EEA member country.

Measures

18.8. The customer is:

a) For PISPs: the customer is the natural or legal person who holds the payment account and requests the initiation of a payment order from that account. In the specific case where the PISP has a business relationship in the meaning of Article 3(13) of Directive (EU) 2015/849 with the payee for offering payment initiation services, and not with the payer, and the payer uses the respective PISP to initiate a single or one-off transaction to the respective payee, the PISPs' customer for the purpose of these Guidelines is the payee, and not the payer. This is without prejudice to Article 11 of Directive (EU) 2015/849 and Title I of these guidelines especially with regards to occasional transactions, and the PISPs' obligations under Directive (EU) 2015/2366 and other applicable EU legislation.

b) For AISPs: the customer is the natural or legal person who has the contract with the AISP. This can be the natural or legal person who holds the payment account(s).

18.9. PISPs and AISPs should take adequate measures to identify and assess the ML/TF risk associated with their business. To this end, PISPs and AISPs should take into account all data available to them. The type of data available to them will depend, *inter alia*, on the specific service offered to the customer, with the explicit consent of the payment service user and which is necessary for the provision of their services, in accordance with Article 66(3), letter (f) and Article 67(2), letter (f) of Directive (EU) 2015/2366.

18.10. Considering Article 11 of Directive (EU) 2015/849, PISPs and AISPs should determine the extent of CDD measures on a risk-sensitive basis, taking into account all data available to them with the explicit consent of the payment service user and which is necessary for the provision of their services, in accordance with Article 66(3), letter (f) and Article 67(2), letter (f) of Directive (EU) 2015/2366. In most cases, the low level of inherent risk associated with these business models means that SDD will be the norm. With regards to those cases of low risk and to the extent the application of SDD measures is prohibited or restricted under national law, AISPs and PISPs may adjust their CDD measures and apply guideline 18.15 accordingly.

18.11. Monitoring: As part of their CDD processes, PISPs and AISPs should ensure that their AML/CFT systems are set up in a way that alerts them to unusual or suspicious transactional activity, taking into account all data available to them with the explicit consent of the payment service user and which is necessary for the provision of their services, in accordance with Article 66(3), letter (f) and Article 67(2), letter (f) of Directive (EU) 2015/2366. PISPs and AISPs should use their own, or third party typologies, to detect unusual transactional activity.

Customer due diligence

18.12. PISPs and AISPs should apply the CDD measures to their customers in line with Title I.

18.13. Pursuant to Article 13 of Directive (EU) 2015/849 each time an account is added, the AISP should ask the customer, or verify through other means, whether the account is his own account, a shared account, or a legal entity's account for which the customer has a mandate to access (e.g.: an association, a corporate account).

Enhanced customer due diligence

18.14. In higher risk situations, firms should apply the EDD measures set out in Title I.

Simplified customer due diligence

18.15. Firms should always know the name of their customer. PISPs and AISPs and may consider applying SDD such as:

a) Relying on the source of funds as evidence of the customer's identity where the payment account details of the customer are known, and the payment account is held at an EEA-regulated payment service provider;

b) Postponing the verification of the customer's identity to a certain later date after the establishment of the relationship. In that case, firms should ensure that their policies and procedures set out at what point CDD should be applied;

c) Assuming the nature and purpose of the business relationship;

Guideline 19: Sectoral guideline for firms providing activities of currency exchange offices

19.1. Firms providing currency exchange services should take into account, together with Title I, the provisions referred to in this Guideline.

19.2. Firms should have regard to the inherent risks of the currency exchange services which may expose them to significant ML/TF risks. Firms should be aware that these risks stem from the simplicity of transactions, their speed and their often cash-based character. Firms should also have regard to the fact that their understanding of the ML/TF risk associated with the customer may be limited due to the fact that they usually carry out occasional transactions rather than establish a business relationship.

Risk factors

Product, service and transaction risk factors

19.3. Firms should take into account the following factors as potentially contributing to increased risk:

a) The transaction is unusually large in absolute terms or compared with the economic profile of the customer;

b) The transaction has no apparent economic or financial purpose;

19.4. Firms should take into account the following factors as potentially contributing to reduced risk:

a) The amount changed is low; firms should note that low amounts alone will not be enough to discount TF risk;

Customer risk factors

19.5. Firms should take into account the following factors as potentially contributing to increased risk:

a) The customer behaviour :

i. the customer's transactions are just below the applicable threshold for CDD, in particular where these are frequent or within a short period of time;

ii. the customer cannot or will not provide information about the origin of the funds;

iii. the customer requests to exchange large amounts of foreign currency which is not convertible or not frequently used;

iv. the customer exchanges large quantities of low denomination notes in one currency for higher denominations notes in another currency; or vice versa.

v. The customer's behaviour makes no apparent economic sense;

vi. The customer visits many premises of the same firm in the same day (To the extent that it is known by the firm);

vii. The customer enquiries about identification threshold and/or refuses to answer casual or routine questions;

viii. The customer converts funds of one foreign currency into another foreign currency;

ix. Exchange of large amounts or frequent exchanges that are not related to the customer's business;

x. The currency sold by the customer is inconsistent with his or her country of citizenship or residence;

xi. The customer buys currency from an unusual location in comparison to his/her own location without any logical explanation;

xii. The customer buys currency that does not fit with what is known about the customer's country of destination;

xiii. The customer buys or sells a large amount of a currency from a jurisdiction associated with significant levels of predicate offences to ML or terrorist activity;

b) The customer's business activity:

i. The customer business is associated with a higher ML/TF risk for example casinos, purchase/sale of precious metal and precious stones, scrap dealer;

Distribution channel risk factors

19.6. Firms should take into account the following factors as potentially contributing to increased risk:

a) The service is provided entirely online without adequate safeguards;

b) The provision of services is conducted through an agent network

Country or geographical risk factors

19.7. Firms should take into account the following factors as potentially contributing to increased risk:

a) The bureau de change business is located in a jurisdiction associated with higher ML/TF risk;

Measures

19.8. Since this business is primarily transaction-based, firms should consider which monitoring systems and controls they put in place to ensure that they are able to detect money-laundering and terrorist financing attempts, even where the CDD information they hold on the customer is basic or missing. This monitoring system should be adapted to the business volume and the risk exposure.

Customers due diligence

19.9. Firms should clearly define in their internal policies and procedures at what point they should carry out CDD to their occasional customers. This should encompass:

a) The situation where a transaction or identified linked transactions amount to EUR 15 000, or to the national threshold(s) if lower, or more. The policies and procedures should clearly define at what point a series of one-off transactions amounts to a business relationship taking into account the context of the firms'activities (i.e. the average normal size of a one-off transaction by their normal clientele).

b) The situation where there is a suspicion of money laundering or terrorist financing.

19.10. Firms should in any case put in place systems and controls in accordance with guideline 4.7 (b) to:

a) identify linked transactions (for example, to detect whether the same customer approaches multiple offices in a short space of time);

b) monitor transactions in a way that is adequate and effective in light to the size of the firm, the number of its offices, the size and volume of transactions; the type of activities performed, its delivery channels and the risks identified in its business-wide risk assessment.

Enhanced customer due diligence

19.11. Where the risk associated with an occasional transaction or business relationship is increased, firms should apply EDD in line with Title I, including, where appropriate, increased

transaction monitoring (e.g. increased frequency or lower thresholds), obtaining more information about the nature and purpose of the business, or the source of the customer's funds.

Simplified customer due diligence

19.12. To the extent permitted by national legislation, firms may consider applying SDD in low- risk situations such as:

a) postponing the verification of the customer's identity to a certain later date after the establishment of the relationship.

b) verifying the customer's identity on the basis of a payment drawn on an account in the sole or joint name of the customer with an EEA-regulated credit or financial institution.

Guideline 20: Sectoral guideline for corporate finance

20.1. Firms providing corporate finance services should take into account the inherent ML/TF risks linked with these activities and be mindful that such activity is based on close advisory relationships in particular with corporate clients and other parties such as potential strategic investors.

20.2. When offering corporate finance services, firms should apply Title I and additionally the provisions set out in this Guideline. The sectoral guidelines 12, 15 and 16 may also be relevant in this context.

Risk factors

Customer and beneficiary risk factors

20.3. Where offering corporate finance services, firms should take into account the following risk factors as potentially contributing to increased risk:

a) the ownership of the customer is opaque without any obvious commercial or lawful rationale. For example, where ownership or control is vested in other entities such as trusts or Securitisation special purpose entities as defined in Article 2(2) of Regulation (EU) 2017/2402 (SSPE);

b) corporate structures or transactions are complex such as a long holding chain with use of front companies, or a lack transparency, and this appears to be for no reasonable business purpose;

c) where there is no evidence the customer has received a mandate or a sufficiently senior management approval to conclude the contract;

d) there are few independent means of verification of the customer's identity;

e) misconduct such as securities fraud or insider trading is suspected.

20.4. Where offering corporate finance services, firms should take into account the following risk factors as potentially contributing to reduced risk. The customer is:

a. a public administration or enterprise from a jurisdiction with low levels of corruption; or

b. a credit or financial institution from a jurisdiction with an effective AML/CFT regime, and is supervised for compliance with their AML/CFT obligations.

Country or geographical risk factors

20.5. Where offering corporate finance services, firms should take into account the following risk factors as potentially contributing to increased risk:

a. the customer or their beneficial owner is based in, or associated with, jurisdictions associated with higher ML/TF risk. Firms should pay particular attention to jurisdictions with high levels of corruption.

Measures

20.6. Providers of corporate finance will, by the nature of the business, be gathering substantial due diligence information as a matter of course; firms should draw upon this information for AML/CFT purposes.

Enhanced customer due diligence

20.7. Where the risk associated with a business relationship or an occasional transaction is increased, firms should apply EDD measures such as:

a) Additional checks on customers' ownership and control structure, beneficial ownership, and in particular any links the customer might have with politically exposed persons, and the extent to which these links affect the ML/TF risk associated with the business relationship;

b) Assessments of the integrity of directors, shareholders, and other parties with significant involvement in the customer's business and the corporate finance transaction;

c) Verification of the identity of other owners or controllers of a corporate entity;

d) Establishing the source and nature of the funds or assets involved by all the parties to the transaction, where appropriate through evidence or assurances from appropriate third parties.

e) Additional checks in order to establish the financial situation of the corporate client;

f) Use of non-documentary forms of evidence, such as meetings with credible persons who know the individuals in question; such as bankers, auditors or legal advisors. Firms should consider if this evidence is sufficient to demonstrate that the customer has correctly represented their personal and financial circumstances. Where non-documentary evidence of this sort is used, a record setting out the basis on which decisions were reached should be kept;

g) Risk-sensitive customer due diligence checks on other parties to a financial arrangement to gain sufficient background knowledge to understand the nature of the transaction. This is because money laundering risks may be posed to the firm not only by its customers, but also by parties to transactions with whom the firm does not have a direct business relationship. Firms should have regard to the fact that those parties may include:

i. the take-over or merger target of a client firm;

ii. potential or actual investors in a corporate client;

iii. corporate entities in which the firm takes a substantial ownership stake (but with which it does not have a wider business relationship);

iv. potential future customers;

v. in securitization transactions as defined in Article 2(1) of Regulation (EU) 2017/2402: agents acting on behalf of the SSPE (who may or may not be a regulated entity);

h) Firms offering corporate finance services should apply enhanced ongoing monitoring. In that regard, firms that use automated transaction monitoring should combined it with the knowledge and expertise of staff engaged in the activity. This enhanced monitoring should result in a clear understanding of why a customer undertakes a particular transaction or activity; for this purpose, firms should ensure that their staff use their knowledge of the customer, and what would be normal in the given set of circumstances, to be able to spot the unusual or potentially suspicious.

i) When taking part in securities' issuance, the firm should confirm that third-parties participating in selling securitisation instruments or transactions to investors have sufficient customer due diligence arrangements of their own in place.

j) In considering the ML/TF risks associated with a securitisation instruments or transaction, a firm should understand the underlying economic purpose of the arrangement, including the level of due diligence appropriate for different parties to the arrangement, which may include parties with whom the firm does not have a direct business relationship .

Simplified due diligence (SDD)

20.8. Firms should use the information they have thanks to the relationship-based nature of corporate finance activity, the scale of the transactions, and the need to assess credit risk and reputational risk posed by corporate finance arrangements also for SDD purposes.

20.9. Where firms are dealing with intermediaries who maintain accounts for the primary benefit of their underlying customers, firms should apply sectoral guideline 16.

4. Accompanying documents

4.1 Cost-benefit analysis/impact assessment

Introduction

1. Directive (EU) 2015/849 places the risk-based approach at the center of the Union's AML/CFT regime. The risk of ML/TF can vary and a risk-based approach helps effectively to manage that risk. Credit and financial institutions ('firms') need to identify and understand the details of their customers as a central point to the risk based-approach in this process.

2. Directive (EU) 2015/849 requires the ESAs to issue guidelines ('GL') 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 (CDD) would be appropriate. The aim is to promote a common understanding, by firms and competent authorities, of what the risk-based approach to AML/CFT entails and how it should be applied. These Guidelines were published in 2017[21].

3. On 19 June 2018, Directive (EU) 2018/843 entered into force. This Directive amends Directive (EU) 2015/849 to strengthen the fight against terrorist finance and ensure the increased transparency of financial transactions. As a result, these Guidelines have to be updated to take account of the new legal framework.

4. At the same time, the ESAs' ongoing work on ML/TF risk highlighted several areas where significant differences continue to exist in firms' approaches to AML/CFT (e.g. COM's Supranational Risk Assessment Report with specific ESA's recommendations, the ESA's Opinion on the use of innovative solutions in the customer due diligence process, the ESA's Joint Opinions on the risks of ML/TF affecting the European Union's financial sector). As a result, it appears necessary to provide more details to existing central parts of the guidelines (e.g. business-wide and individual risk assessments, CDD, identification of the beneficial owner). These Guidelines have to clarify the supervisory expectations on those points.

5. Moreover, since the first publication of these Guidelines in 2017, the financial sector has evolved and existing and emerging risks have been identified (e.g. crowdfunding platforms, Payment Initiation Service Providers (PISPs) and Account Information Service Providers (AISPs), firms providing activities of currency exchange offices, corporate finance). Therefore, new sectoral guidelines have to be included so as to tackle the specific AML/CFT risks of those sectors and to promote convergence.

[21] The Risk Factors Guidelines

Scope and objectives

6. This impact assessment describes the policy options the ESAs considered when drafting a revised version of these guidelines and sets out how these policy options might affect their stakeholders.

7. For the new impact assessment, the ESAs considered the views of AML/CFT competent authorities, previous cost-benefit analyses and the Commission Staff's impact assessment of its proposal for a fifth Anti-Money Laundering Directive, and the ESAs' 2019 Joint Opinion on the ML/TF risk affecting the EU's financial sector.

8. The ESAs' impact assessment considered the additional details that were incorporated in the revised guidelines addressing new risks, namely: business-wide and individual ML/TF risk assessments; financial inclusion, occasional transactions, customer due diligence measures; identification of the beneficial owner including of a public administration or a state-owned enterprises, terrorist financing risk factors; and new guidance on emerging risks, such as the use of innovative solutions for CDD purposes. The ESAs' impact assessment also considered the sectoral guidelines.

9. The ESAs found that the application of these revised guidelines addressing new risks and covering additional sectors would not give rise to significant costs over and above those that firms and competent authorities would incur as a result of the underlying legal obligations set out in Directive (EU) 2015/849.

10. 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 revised guidelines by competent authorities and firms. Instead, this impact assessment examines, in qualitative terms, the impact that these revised guidelines would have if all firms and competent authorities fully complied with them. This means that the estimated net impact of the preferred options should be interpreted as the maximum impact of the full implementation of the proposed revised guidelines. The impact of the actual implementation of these revised guidelines could be less.

Baseline

11. Regarding simplified customer due diligence (SDD), Article 17 of Directive (EU) 2015/849 requires the ESAs to issue guidelines on:

    - the risk factors to be taken into consideration; and

    - the measures to be taken in situations where SDD measures are appropriate.

12. Regarding enhanced customer due diligence (EDD), Article 18(4) of Directive (EU) 2015/849 requires the ESAs to issue guidelines on:

- the risk factors to be taken into consideration; and

- the measures to be taken in situations where EDD measures are appropriate.

13. In both cases, SDD and EDD, the ESAs have to take specific account of the nature and size of firms' business.

14. For the impact assessment, the ESAs considered options in relation to:

- the consistency of these guidelines with international AML/CFT standards (3 options); and

- the level of prescription (2 options).

Consistency with international AML/CFT standards

15. Guidance has been published by international standard setters, including the FATF and the Basel Committee on Banking Supervision. There are three options to consider, taking into account possible advantages and disadvantages: 1) ESAs' GL simply reproduce international AML/CFT standards; 2) ESAs' GL consistent with international AML/CFT standards; or 3) ESAs' GL disregard international AML/CFT standards.

Option 1 – ESAs' GL simply reproduce international AML/CFT standards

16. The ESAs' guidelines could reproduce, or simply refer to, international standards and guidance on ML/TF risk factors and simplified and enhanced CDD.

17. The advantage of simply reproducing international AML/CFT standards is that it consolidates existing guidance and makes compliance easier for firms with an international footprint.

18. The disadvantage of simply reproducing international AML/CFT standards is that it is insufficient to meet the requirements of Articles 17 and 18(4) of amended Directive (EU) 2015/849.

19. The international AML/CFT standards do not:

- take into account specific measures set out in the amended Directive (EU) 2015/849 to address new risks, for example in relation to firms' identification, assessment of business-wide risk and the risk associated with individual business relationships, certain electronic money products or high-risk third countries that have been identified by the European Commission as posing significant risks to the European Union's financial system;

- cover all the financial sectors included in amended Directive (EU) 2015/849's scope; or

- contain sufficient detail to ensure the consistent application of Directive (EU) 2015/849's risk-based approach as for instance no Risk Based Approach (RBA) international guidance has been elaborated for AISPs and PISPs or corporate finance.

20. There are additional elements that need to be taken into account such as:

    - a need for a clear and coordinated customer due diligence requirements including on a non-face to face basis;

    - for a better monitoring of transactions involving high-risk third countries; and

    - access to updated beneficial ownership information in relation to corporate and legal arrangements.

Option 2 – ESAs' GL are consistent with international AML/CFT standards

21. The ESAs' Guidelines could be drafted in a way that is consistent with existing international standards and guidance.

22. The advantage of this approach is that it allows the ESAs to address provisions that are specific to Directive (EU) 2015/849 and tailor their approach to those financial sectors within Directive (EU) 2015/849's scope. It also allows the drafting of the guidelines in a way that is conducive to the consistent and coherent application of the risk-based approach by firms and competent authorities across the EU.

23. 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 - ESAs' GL disregard international AML/CFT standards

24. The ESAs' guidelines could be drafted without regard to international standards and guidance.

25. The advantage of this approach is that it allows the ESAs to issue guidelines specific to the European context.

26. The disadvantage of this approach is that it risks exposing Member States to international censure should their approach be in breach of international standards.

Preferred option

27. Option 2 is the ESAs' preferred option because it allows firms and competent authorities to comply with international standards and guidelines while fostering the consistent and coherent application of the risk-based approach across the EU.

Level of prescription

28. Directive (EU) 2015/849 identifies a number of specific cases that firms must always treat as high risk. For enhanced customer due diligence, for instance: i) where the customer, or the customer's beneficial owner, is a PEP; ii) where a firm enters into a correspondent relationship involving the execution of payments with a third-country respondent institution; iii) where a business relationship or a transaction involves a high-risk third country; and iv) all transactions that are complex, unusually large, conducted in an unusual pattern; or without obvious economic or lawful purpose. In some cases, Directive (EU) 2015/849 prescribes what firms must do to mitigate that risk.

29. However, most of Directive (EU) 2015/849 contains only high-level principles and obligations.

Option 1 – Exact definitions and actions (what constitutes high ML/TF risk and low ML/TF risk and what firms should do)

30. The guidelines could set out exactly what constitutes high and low risk for each specific case mentioned in the Directive (EU) 2015/849 and what firms should do in each of these cases.

31. There are some advantages. 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.

32. There are some disadvantages to consider. This approach is unlikely to be proportionate or effective, as firms and competent authorities will focus on formal compliance rather than the successful identification, assessment and management of ML/TF risk in substance. This approach also fails to take account of contextual factors that could move a business relationship or occasional transaction into a higher or lower risk category. For example, setting monetary thresholds below which a relationship should be considered low risk at European level may lead to the application of inadequate risk mitigation measures in jurisdictions where this threshold does not reflect average incomes. There is also a risk that prescribing high- and low-risk situations will lead to firms failing to identify and manage high-risk situations that are not set out in the guidelines (for instance, from new factors and contexts not addressed in the high level of prescription). Finally, this approach is not compatible with international AML/CFT standards and guidance.

Option 2 – Information to consider (to assess as high or low ML/TF risk, and which type of CDD might be appropriate to manage that risk)

33. The guidelines could provide firms with information on what they need to consider when determining whether a situation presents a high or a low ML/TF risk, and which type of CDD (simplified or enhanced) might be appropriate to manage that risk.

34. There are some advantages. This approach allows firms to develop a good understanding of the ML/TF risk to which they are exposed. It also enables firms to focus their resources on areas of high-risk, which is conducive to the adoption of proportionate and effective AML/CFT controls.

35. The disadvantage of this approach is that it requires firms and competent authorities to increase their costs to achieve and maintain a sufficient AML/CFT expertise to identify, assess and manage ML/TF risk effectively in order to risk-assess individual business relationships or occasional transactions (instead of just a high level of prescriptive factors to follow).

Preferred option

36. 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

37. The ESAs' preferred options are guidelines that:

    - are consistent with relevant international standards and guidance;

    - provide firms with the information they need to identify, assess and manage ML/TF risk in a proportionate and effective manner.

38. The ESAs expect firms and competent authorities to incur at times significant costs as they review and make changes to their approaches to comply with new national legal frameworks resulting from the transposition of the amended 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.

39. This means that these guidelines should not create significant costs for firms or competent authorities above those associated with a move to the legal AML/CFT regime under the amended 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

40. The benefits 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. Smaller institutions with less complex activities will need to continue to maintain qualified staff and procedures that are proportionate to the ML/TF risk incurred. 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.

41. All firms will face some one-off costs as a result of reviewing their internal policies and controls, making necessary adjustments to reflect these guidelines and training staff accordingly. There are additional details in the revised guidelines addressing new risks as described above that need to be assimilated into the regular procedures of the firms. The one-off costs will be higher for firms with more complex activities and firms that do not already apply a risk-based approach as they should have already done.

42. However, these one-off costs are likely to be offset by all firms in the medium to long term once the necessary adjustments have been made. Furthermore, and based on previous impact assessments, since these adjustments are likely to take place at the same time as legislation transposing amended Directive (EU) 2015/849 come into effect. Therefore, 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 legal and regulatory obligations. This means that the costs attributable to these guidelines, namely due to updates in internal documentation and additional tasks and training for some staff will not in the end be significant.

43. In light of the considerations regarding costs and benefits set out above, the net impact of these Guidelines for firms is likely to be close to zero.

Competent authorities

44. The benefits of this approach for competent authorities are that the guidelines will help supervisors to communicate and set clear expectations of the factors firms should consider when identifying and assessing ML/TF risk and deciding on the appropriate level of CDD.

45. The costs to competent authorities will arise mainly from reviewing existing regulatory guidance to firms and supervisory manuals to ensure consistency with these guidelines. Competent authorities will also incur some costs from additional tasks for specialist AML/CFT risk experts and risk staff with ML/TF risks as part of their wider responsibilities with influence in the off-site and on-site activities, in particular for the supervision of payment service providers and e-money institutions, and retraining of ML/TF staff in general. However, all of these costs are likely to be one-off costs that are likely to be absorbed as part of their on-going work by competent authorities as they are already supposed to enforce a risk-based approach for ML/TF risks. The one-off costs will be higher for competent authorities that are unfamiliar

with the risk-based approach for ML/TF risks. There could be significant costs accruing in those jurisdictions where the banks and authorities rely on simple systems and the existing compliance functions are limited in size, but they are unlikely to exceed the costs arising from the implementation of national legislation, namely transposing the amended Directive (EU) 2015/849.

46. In light of the considerations regarding costs and benefits set out above, the net impact of these guidelines for competent authorities is expected to be close to zero, but positive.

4.2 Overview of questions for consultation

Question 1: Do you have any comments on the proposed changes to the Definitions section of the Guidelines?

Question 2: Do you have any comments on the proposed amendments to Guideline 1 on risk assessment?

Question 3: Do you have any comments on the proposed amendments to Guideline 2 on identifying ML/TF risk factors?

Question 4: Do you have any comments on the proposed amendments and additions in Guideline 4 on CCD measures to be applied by all firms?

Question 5: Do you have any comments on the amendments to Guideline 5 on record keeping?

Question 6: Do you have any comments on Guideline 6 on training?

Question 7: Do you have any comments on the amendments to Guideline 7 on reviewing effectiveness?

Question 8: Do you have any comments on the proposed amendments to Guideline 8 for correspondent banks?

Question 9: Do you have any comments on the proposed amendments to Guideline 9 for retail banks?

Question 10: Do you have any comments on the proposed amendments to Guideline 10 for electronic money issuers?

Question 11: Do you have any comments on the proposed amendments to Guideline 11 for money remitters?

Question 12: Do you have any comments on the proposed amendments to Guideline 12 for wealth management?

Question 13: Do you have any comments on the proposed amendments to Guideline 13 for trade finance providers?

Question 14: Do you have any comments on the proposed amendments to Guideline 14 for life insurance undertakings?

Question 15: Do you have any comments on the proposed amendments to Guideline 15 for investment firms?

Question 16: Do you have any comments on the proposed amendments to Guideline 16 for providers of investment funds and the definition of customer in this Guideline?

Question 17: Do you have any comments on the additional sector-specific Guideline 17 on crowdfunding platforms?

Question 18: Do you have any comments on the additional sector-specific Guideline 18 on account information and payment initiation service providers?

Question 19: Do you have any comments on the additional sector-specific Guideline 19 on currency exchanges?

Question 20: Do you have any comments on the additional sector-specific Guideline 20 on corporate finance?

4.3 Summary of responses to the consultation and the EBA's analysis

The EBA notes that it has received a substantial number of comments that do not relate to any revision to the Guidelines proposed in the Consultation Paper. Taking into account the limited scope of the consultation as announced in the Consultation Paper (JC 2019 87), the EBA has only briefly summarized such suggestions below for each Guideline and may consider them when preparing future revisions of these Guidelines.

The EBA has used the opportunity of the revision of the Guidelines to make a number of editorial amendments. Those editorial amendments are not listed in the feedback table below.

Guideline	Summary of responses received	EBA analysis	Amendments to the proposal
Feedback on the general comments			
General comment	One respondent suggested that the Legal Entity Identifier should be used in all customer due diligence processes.	Given that Directive (EU) 2015/849 (AMLD) does not contain the requirement for firms to obtain Legal Entity Identifiers (LEIs), the EBA does not require their usage in these Guidelines either. However, the EBA acknowledges that a further increased use of LEIs can potentially support the fight against ML and TF, both during on-boarding and subsequent monitoring of the business relationship and associated transactions to detect suspicious transactions, and might help making the application of CDD measures more efficient. That said, the use of LEIs is not enough, by itself, to meet financial institutions' CDD obligations as the information contained in LEIs falls short of that required for CDD purposes, and because institutions remain ultimately responsible for any failure to meet their obligations under Article 13 of the AMLD.	*None*
General comment	One respondent proposed to add to the guidelines a numerical value to measure the inherent risk.	The assessment of ML/TF risk is a complex process that differs significantly between firms in terms of types of risks to consider and the weight to attach to each of them. The EBA does not consider it suitable to reduce such an assessment to a single numerical value, nor does it subscribe to the alleged comparability of such a value across firms. More guidance on how to assess ML/TF risks is provided in guideline 3.	*None*

General comment	One respondent was of the view that the EBA should foster a more common industry approach to identifying, addressing and managing customer and third-party risk, and that the final guidelines should reflect, where possible, this approach in line with FATF Recommendation 10 to ensure international consistency.	The guidelines proposed in the Consultation Paper take into account FATF recommendations and contain requirements regarding the identification and assessment of ML/TF risk. More specifically, the guidelines require that firms identify and manage, inter alia, customer risk and third-party related ML/TF risk. The EBA took into account international standards, such as FATF recommendation 10 on customer due diligence, when drafting the guidelines. At the same time, the EBA notes that due to the minimum harmonization nature of the AMLD and existing divergence between national legislation, there is room for further harmonisation and international consistency. This is also what the EBA has recently advised in respect of a future legal framework in the EU on AML/CFT (see EBA/OP/2020/14 and EBA/REP/2020/25).	*None*
General comment	One respondent commented that there was a risk that firms and AML/CFT supervisors might follow different approaches in respect of customers that may possess 'golden visas'. This respondent also mentioned that the topic of access to 'citizenship by investment' and 'residency by investment' schemes ('residency visas') was discussed extensively by the European Parliament's Special Committee on financial crimes, tax evasion and tax avoidance (TAX3). One respondent called for the EBA to include more guidance on investment citizenship schemes or 'golden visas' in the Guidelines and asked to include a specific reference to OECD publications that firms could use as possible source of information in Guideline 1.30.	The EBA notes that the topic of 'golden visas' and 'residency visas' itself is out of scope of the Risk Factors Guidelines. In relation to the investment citizenship schemes, the EBA takes note of the actions recently taken by the co-legislators, but does not see grounds to amend the Guidelines, as the EBA considers these risks to fall under the broader categories of customer risk, country or geographical risks and the guidelines, in particular guideline 2, already contain requirements in this regard. With regard to the OECD publications, the EBA strongly supports and promotes that firms use publicly available information and knowhow, including publications by intergovernmental organizations. As OECD highlights on its website, there are substantial similarities between the techniques used to launder the proceeds of crimes and to commit tax crimes. It is key for supervisors and firms to enhance their understanding of tax crimes, which the EBA has also stressed in several products, more in particular the Report on competent authorities' approaches to tackling market integrity risks associated with dividend arbitrage schemes (EBA/REP/2020/15), the action plan on dividend arbitrage trading schemes and the revised Internal Governance Guidelines (as per the recent Consultation Paper,	*None*

		EBA/CP/2020/20). At the same time, in the EBA's view, Guideline 1.30 and 1.31 include a sufficiently comprehensive list of sources of information to identify ML/TF risk factors and the list is of a non-exhaustive nature.	
Response out of scope	With regards to Guideline 3, one respondent mentioned that different weights should be applied on different risk factors, considering the vulnerability or degree of exposure of the entity to the risk factor, and the severity of the possible impact or damage.	The suggestion is not related to any of the revisions to the guidelines that was proposed in the CP and therefore out of scope of the consultation.	*None*
Feedback on responses to Question 1 (Definitions)			
Definitions	Many respondents requested to amend the proposed definition of 'non-face to face relationships or transactions', arguing that the use of video-link or similar technological means should be considered as equivalent to face-to-face or, at least, as mitigating the risk of 'non-face to face relationships or transactions'. The respondents referred to FATF guidance and to Annex III of AMLD, to guideline 4.31 and practices in Member States that do not consider the use of video means to imply a higher ML/TF risk per se. Moreover, respondents pointed out the increased use of and the need for such technological means, in particular in the context of the Covid-19 pandemic. Several respondents suggested that greater precision should be provided on potential residual risks in a video identification situation, and on how to mitigate these risks, especially by referring to existing FATF guidance.	The definition section provides a common understanding of relevant terms that are used throughout the Risk Factors Guidelines. This section does not provide any policy consideration in the context of ML/TF risks. For the purpose of these guidelines, 'non-face to face relationships or transactions' means any transaction or relationship where the customer is not physically present, that is, in the same physical location as the firm or a person acting on the firm's behalf. This includes situations where the customer's identity is being verified via video-link or similar technological means. Guideline 2.21 a) i) requires the firm to take into account whether the customer is physically present for identification purposes. Guidelines 4.29 to 4.31 contain requirements on non-face to face situations. In particular, guideline 4.31 states that the use of electronic means of identification does not of itself give rise to increased ML/TF risk, in particular where these electronic means provide a high level of assurance under Regulation (EU) 910/2014. Furthermore, Guideline 4.29 b) clarifies that firms should assess whether the non-face to face nature of the relationship or occasional transaction gives rise to increased ML/TF risk and, if so, adjust their CDD measures accordingly. Also, firms should apply guidelines 4.32 to 4.37 when using innovative technological means to verify identity.	*None*

		The European Commission recently invited the EBA to draft guidelines, in 2021, on elements related to customer remote on-boarding and reliance on customer due diligence processes carried out by third parties. The EBA will publish draft requirements for public consultation in due course.	
Definitions	Several respondents considered that 'high-risk third countries' referred to in Article 9 of AMLD should not be excluded from the definition of 'jurisdictions associated with higher ML/TF risk', or that it should be, at least, clarified that 'jurisdictions associated with higher ML/TF risk' could be of lower risk than 'high-risk third countries' One respondent argued that the EU authorities should provide a list of 'jurisdictions associated with higher ML/TF risk' to ensure harmonized application among member states.	'Jurisdictions associated with higher ML/TF risk' means countries that, based on an assessment by obliged entities of the risk factors set out in Title I of these guidelines, present a higher ML/TF risk. In particular, Guidelines 2.9 to 2.15 contain requirements on how firms themselves should assess ML/TF risks associated with countries and geographical areas. Guideline 4.62 clarifies that obliged entities, in high-risk situations, need to take an informed decision about which EDD measures are appropriate. The term 'jurisdictions associated with higher M:/TF risk' excludes 'high-risk third countries' that are identified and publicly listed by the European Commission as having strategic deficiencies in their AML/CFT regime, which pose a significant threat to the Union's financial system (Article 9 of AMLD). The AMLD requires specific EDD measures to be applied in the context of high-risk third-countries. The amendment in the definition is aimed at better distinguishing 'high-risk third countries' from the 'jurisdictions associated with higher ML/TF risk'. The general assumption made by respondents that 'jurisdictions associated with higher ML/TF risk' imply, to some extent, a lower ML/TF risk than 'high-risk third countries' is not reasonable.	*None*
Definitions	One respondent proposed to add a definition of 'jurisdictions associated with lower ML/TF risk'.	Guideline 2.12 is sufficiently clear. To the extent permitted by national legislation, firms should be able to identify lower risk jurisdictions in line with these guidelines and Annex II of AMLD.	*None*
Definitions	One respondent suggested that a definition of 'high-risk third countries' should be added and that the use of the term 'country' should be restricted to these guidelines while the terms 'jurisdictions' and 'geographies' should be used in other guideline, to avoid misinterpretation.	The term 'high-risk third countries' is defined in Article 9(1) of AMLD and is therefore also used in these Guidelines where applicable. The Guidelines additionally refer to 'countries', 'jurisdictions' and 'geographical area' as and when appropriate, taking into account	*None*

		the specific meaning of each term. For example, the term 'geographical area' could include a number of countries.	
Definitions	Several respondents proposed to modify the definition of 'risk appetite' to align the expression with the definition in EBA guidelines on internal governance. One respondent suggested that a definition of 'risk appetite statement' should be added as follows: 'The articulation in written form of the aggregate level and types of risk that a financial institution is willing to accept, or to avoid, in order to achieve its business objectives.'. This respondent also proposes to replace the term 'risk appetite' by 'risk appetite statement' in Guideline 4.7 g). One respondent suggested that the guidelines should indicate the difference between 'risk appetite' and 'risk tolerance' as supervisory authorities would not use both terms consistently.	The 2020 Consultation Paper on a revised version of the EBA Internal Governance Guidelines (EBA/CP/2020/20) defines risk appetite, for prudential purposes, as 'the aggregate level and types of risk a firm is willing to assume within its risk capacity, in line with its business model, to achieve its strategic objectives.' The different definition included in the draft revised Risk Factors Guidelines of the term 'risk appetite' as 'the level of risk a firm is prepared to accept' is appropriate, recognising that the focus of the Risk Factors Guidelines is ML/TF risk. The EBA does therefore not see a need for inclusion of a separate term 'risk appetite statement' given that Guideline 4.7(g) states that 'Firms should set out clearly, in their policies and procedures, (…) the firm's risk appetite'. The EBA also notes that the term 'risk appetite' is defined in the Guidelines while the term 'risk tolerance' is not used.	*None*
Definitions	One respondent suggested that a definition of 'risk' should be added, as 'the possibility of ML/TF taking place'.	The definitions section of the Risk Factors Guidelines already contains the term 'risk' meaning 'the impact and likelihood of ML/TF taking place'.	*None*
Definitions	One respondent proposed to add a definition of 'individual risk assessment'.	Guidelines 1.9 b) i) and 1.20 to 1.22 give sufficient clarity of what an individual risk assessment is composed of.	*None*
Definitions	One respondent suggested that a definition of 'correspondent banking relationship' and 'respondent banking relationship' should be added in the Definitions section.	The term 'correspondent relationship' is defined in Article 3(8) of AMLD, including references to the 'correspondent' and the 'respondent'. Guideline 8.1 refers to this definition. Guideline 8.2 contains further clarification on the term. An additional definition of a 'respondent banking relationship' is therefore not necessary.	*None*
Definitions	One respondent proposed to add a definition of 'senior managing official'	The term 'senior managing official' is of relevance with regards to the identifying beneficial owners. Obliged entities should identify the customer's beneficial owner as defined in Article 3(6) AMLD. Guideline 4.20 further clarifies when and how to identify the customer's senior managing official(s) as beneficial owner(s). Guideline 4.21 requires that, when deciding which senior	*None*

		managing official(s) to identify as beneficial owner, firms should consider who has ultimate and overall responsibility for the customer and take binding decisions on the customer's behalf. As there are differences in corporate structures among Member States, the addition of a more specific definition of the term 'senior managing official' that is relevant in each case would not be feasible.	
Definitions	One respondent asked to clarify that 'should' has the same meaning as 'must'.	By way of convention, the terms 'shall' and 'must' are used (interchangeably) for requirements that are set out in EU Directives and Regulations, including in regulatory technical standards of the EBA, whereas the term 'should' is used for requirements that are set out for example in EBA Guidelines.	*None*
Definitions	One respondent proposes to add a definition of 'outsourcing'.	Outsourcing is defined in the EBA Guidelines on outsourcing arrangements (EBA/GL/2019/02), meaning 'an arrangement of any form between an institution, a payment institution or an electronic money institution and a service provider by which that service provider performs a process, a service or an activity that would otherwise be undertaken by the institution, the payment institution or the electronic money institution itself'. Guidelines 2.21 f) and 4.34 include references to outsourcing arrangements and, in particular to the aforementioned EBA Guidelines on outsourcing arrangements. Those GLs are applicable to credit institutions, investment firms, payment institutions and electronic money institutions. For the purposes of the Risk Factors Guidelines, the addition of an 'outsourcing' definition is therefore not necessary.	*None*
Summary of responses out of scope	One respondent suggested that guidance for additional business models/sectors, in particular credit or charge card companies, should be included. One respondent proposed not to use the term 'holistic' and to clarify expectations in the assessment of risk factors associated to a business relationship.	The suggestion is not related to any of the revisions to the guidelines that was proposed in the CP and therefore out of scope of the consultation.	*None*

Feedback on responses to Question 2 (risk assessment)			
Guideline 1.2 a)	One respondent proposed to add the requirement to '[…] obtaining a holistic view' in the context of the business-wide risk assessment.	Guideline 1.26 states that firms should take a holistic view for individual risk assessments. Guideline 3.2 includes the requirement that firms should take a holistic view of the ML/TF risk factors they have identified that, together, will determine the level of ML/TF risk associated with a business relationship, an occasional transaction, or their business. The AMLD refers to a holistic, risk-based approach also at business-wide level. Having assessed the consultation response, the EBA agrees that further clarification on taking a holistic view in the context of business-wide risk assessments would is warranted, and therefore amended guideline 1.12.	*'1.12 To this end, firms should take a holistic view of the ML/TF risks to which they are exposed, by identifying and assessing the ML/TF risk associated with the products and services they offer, the jurisdictions they operate in, the customers they attract and the transaction or delivery channels they use to service their customers.*
Guideline 1.2.c) and d)	One respondent proposed changing 'c)' and 'd)' to '(i)' and '(ii)'.	The EBA, having assessed the consultation response, agrees with the suggestion and has amended the numbering of guideline 1.2.	*'1.2. […]* *Each risk assessment should consist of two distinct but related steps:* *~~c)~~ a) the identification of ML/TF risk factors; and* *~~d)~~ b) the assessment of ML/TF risk.'*
Guideline 1.3	One respondent suggested including the resulting assessment (e.g. accept, avoid or mitigate).	Guideline 1.3 states that, when assessing the overall level of residual ML/TF risk associated with their business and with individual business relationships or occasional transactions, firms should consider both, the level of inherent risk, and the quality of controls and other risk mitigating factors. In this context, the requirements on the firms' risk appetite (1.18, 4.7 g) and 4.64 c)) are of particular relevance. In particular, firms should be able to manage the respective ML/TF risk. Consequently, firms should conclude on how to proceed once the	*None*

		residual risk has been assessed. It might be necessary to further mitigate the ML/TF risk using the provisions in the Risk Factors Guidelines. Guideline 4.66 states that firms should not enter into a business relationship if they are unable to comply with their CDD requirements, if they are not satisfied that the purpose and nature of the business relationship are legitimate or if they are not satisfied that they can effectively manage the risk that they may be used for ML/TF purposes. Where such a business relationship already exists, firms should terminate it or suspend transactions until it can be terminated, subject to instructions from law enforcement, where applicable. Guideline 4.68 requires firms to note that the application of a risk-based approach does not of itself require them to refuse, or terminate, business relationships with entire categories of customers that they associate with higher ML/TF risk, as the risk associated with individual business relationships will vary, even within one category.	
Guideline 1.4	Several respondents suggested that, similar to the FATF guidance on Risk Assessment of February 2013, guideline 1.4 could be expanded to cover who the user of the ML/TF risk assessment is. Many respondents requested further guidance on minimum record keeping requirements as they foresaw this to be an issue with different regulators. Another respondent suggested including the obligation to have the documents available in a digital manner and at least in an English version.	Firms should use the risk assessments in the context of their AML/CFT obligations. Consequently, guideline 1.4 states that firms should record and document their business-wide risk assessment, as well as any changes made to this risk assessment in a way that makes it possible for the firm, and for competent authorities responsible for supervising firms' compliance, to understand how it was conducted, and why it was conducted in a particular way. Further guidance on record-keeping is included in guideline 5. The EBA notes that European law and the Risk Factors Guidelines do not prescribe the format or the language of risk assessments. Firms should take into account any requirements of Member States.	*None*
Guidelines 1.4. and 1.15	One respondent asked for some limitations for credit unions, in relation to reporting and recording requirements.	Guideline 1.16 on proportionality covers this point made by the respondent. Article 8(1) AMLD is clear in this respect.	*None*

Guideline 1.5	Several respondents requested additional clarification which parts of the EBA's Internal Governance Guidelines are of relevance.	A revised version of the EBA Internal Governance Guidelines (EBA/CP/2020/20) that includes a number of references to AML/CFT and ML/TF risk has been publicly consulted in 2020. These requirements provide further clarification in the context of risk assessments.	*None*
Guideline 1.7 a)	Several respondents considered the requirement for an update of the business-wide risk assessment on an annual basis to be very strict and requested more flexibility.	The business-wide risk assessment is a living document. It is crucial that firms update it at least on an annual basis, in a risk sensitive manner. This does not imply that a completely new document needs to be drawn up every year (see also Guideline 1.10).	*None*
Guideline 1.9. b) ii) c)	One respondent proposed including 'new distribution channels' among the risks to be considered by firms when putting into place systems and controls to identify emerging risks in respect of business-wide risk assessments.	The EBA, having assessed the consultation response, agrees with the suggestion. For consistency reasons, the EBA has arrived at the view that the guideline would benefit from similar additions related to other risk factors listed in the AMLD.	*'1.9 b) ii.c): Processes to capture and review information on risks, in particular risks relating to new categories of customers, countries or geographical areas, new products, new services, new distribution channels and new compliance systems and controls.'*
Guideline 1.9 c)	One respondent requested further clarification on the kind of measures expected, and reflected that the type of engagement suggested under guideline 1.9 c) seemed like a commitment outside of the firm's control	In line with common practice, firms should reach out to industry representatives and competent authorities in order to strive for interaction with them as a way to identify emerging risks. Guideline 1.9 c) is clear that firms should put in place processes to feed back the findings, those interaction may have, to relevant staff.	*None*
Guideline 1.10	One respondent suggested deleting reference to the risk-based approach, arguing that risk assessment methodologies are formalised in procedures which updates are performed on a regular basis or upon a trigger event and therefore cannot be done on a risk-sensitive basis.	Guideline 1.7 requires firms to put in place systems and controls to ensure their individual and business-wide risk assessments remain up to date. Furthermore, Guideline 1.10 states that firms should determine the frequency of wholesale reviews of their business-wide and individual risk assessments methodology and that this determination should be performed on a risk-sensitive basis. Firms may also wish to formulate trigger events for wholesale reviews. In any case, firms are expected to assess	*None*

		whether trigger events impact the firm's risk profile and warrant further action.	
Guidelines 1.11 to 1.17	One respondent requested further explanation about how a business-wide risk assessment should be set up and which template should be used.	The guidelines provide requirements on the business-wide risk assessment that are sufficiently flexible to be adapted to any kind of firm and business/nature. Consequently, it would not be appropriate to prescribe a certain template. The EBA also refers to guideline 1.16 on proportionality.	*None*
Guideline 1.15	Several respondents requested further clarification on the word 'unlikely'.	The EBA sets clear requirements on business-wide risk assessments. In particular, 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 (guideline 1.11). Firms should ensure that their business-wide risk assessment is tailored to their business profile and takes into account the factors and risks specific to the firm's business (guideline 1.14). Consequently, the EBA emphasises that a generic ML/TF risk assessment that has not been adapted to the specific needs and business model of the firm ('an off-the-shelf ML/TF risk assessment)', or a group-wide risk assessment that is applied unquestioningly, will in most cases not be enough to meet the requirements in Article 8 of AMLD.	*None*
Guideline 1.17 (b)	One respondent requested to align this guideline with Article 46 AMLD in order to highlight the need for instructions for staff on how they should proceed in such cases.	The Guidelines already refer to Article 46(1) of AMLD.	*None*
Guideline 1.18	Several respondents requested more clarity on the types of 'procedures' which, at a minimum, should be informed by the business-wide risk assessment.	The EBA, having assessed these consultation responses, agrees with the proposal to provide additional clarification. It has therefore amended the guideline to refer to policies, controls and procedures to mitigate and manage effectively ML/TF risks that are explained in Article 8(4) of AMLD.	*'1.18: Firms should use the findings from their business-wide risk assessment to inform their AML/CFT policies, controls and procedures set out in Article 8(3) and (4) of Directive (EU) 2015/849. Firms should ensure that their business-wide risk assessment also reflects the steps taken to assess the ML/TF risk*

			associated with individual business relationships or occasional transactions and their ML/TF risk appetite.'
Guideline 1.18	One respondent argued that the business-wide risk assessment indirectly impacts the individual risk assessment, and asked for further clarification on how the business-wide risk assessment should feed into the individual risk assessment.	Guideline 1.1 requires firms to ensure that they have a thorough understanding of the ML/TF risks to which they are exposed. Firms should therefore perform business-wide and individual risk assessments (Guideline 1.2). Furthermore, Guideline 1.20 states that individual risk assessments should inform, but are no substitute for, a business-wide risk assessment. Furthermore, the EBA expects firms to consider to what extent the ML/TF risks that the firm identified in the business-wide risk assessments are relevant when making individual risk assessments.	*None*
Guidelines 1.18 and 1.19	One respondent requested clarification on how business-wide and individual risk assessments can be linked.	Guidelines 1.18 to 1.20 are clear how the business-wide and individual risk assessments should be linked.	*None*
Guideline 1.19	One respondent reflected that, in the funds industry, the customer risk assessment is more likely to inform the business risk assessment as distinct from the converse.	Guideline 1.20 states that individual risk assessments should inform, but are no substitute for, a business-wide risk assessment.	*None*
Guideline 1.27	One respondent proposed deleting the guideline, arguing that it did not bring any obvious benefit in terms of clarity. One respondent asked the EBA to clarify that there are minimum standards that nevertheless need to be met, e.g. by referring to Guidelines 1.21-1.22.	Guideline 1.27 clarifies, together with guideline 1.26, how to take the holistic view in respect of occasional transactions. Although there is no requirement that firms should draw up a complete customer risk profile for occasional transactions, they nevertheless should conduct the individual risk assessments as required by in guidelines.	*None*
Guideline 1.28	One respondent suggested that it could be useful to look for coherence between Regulation (EU) 2016/679 and AMLD in terms of retention of personal data. One respondent suggested and incorporating this guideline into guideline 4, arguing that firms use data both from on-boarding and throughout the relationship with a customer, as part of their ongoing customer due diligence activities.	With regards to the point on data protection, the EBA refers to Article 41 of AMLD. Guideline 1.28 is explains that information obtained in the course of the business relationship should also be considered for individual risk assessments. Guideline 4 contains monitoring requirements during the business relationship.	*None*

Summary of responses out of scope	1.) With regards to guideline 1.9, several respondents suggested to further reflect aspects of proportionality and the risk-based approach. 2.) With regards to guideline 1.12, one respondent suggested adding '(…) the customers they attract and the transaction and/or delivery channel'. 3.) With regards to guideline 1.16, several respondents suggested amending the second sentence to 'small firms that have limited international or cross border or purely domestic exposure (…)'. 4.) With regards to guideline 1.19, one respondent asked for further clarification about how the business wide risk assessment should inform the initial level of CDD. 5.) With regards to guideline 1.21 and 1.22, one respondent proposed examining whether these two guidelines are necessary when read alongside guideline 2.3, alleging that the concepts described are fully captured in the subsequent guidelines. One respondent suggested replacing 'operate' with 'to which they are exposed' to capture both the idea of 'involving' high risk third countries and third country institutions, as used in guideline 4.46 c) and, in so doing, capture risks associated with jurisdictions who may experience higher level of risks. 6.) With regards to guideline 1.26, two respondents queried the term 'holistic view'. 7.) With regards to guidelines 1.28 to 1.31, one respondent mentioned that some requirements could be burdensome on credit unions. Several respondents provided specific drafting suggestions. 8.) With regards to guideline 1.32, one respondent suggested deleting the reference to the 'number of sources' and specifying that this guideline applies to the business-wide risk assessment.	The suggestion is not related to any of the revisions to the guidelines that was proposed in the CP and therefore out of scope of the consultation.	*None*
Feedback on responses to Question 3 (identifying ML/TF risk factors)			

Guideline 2	Several respondents considered that the guidelines lack of focus on the review and practical application of patterns/typologies and investigative methods, and may be too basic to actually identify sophisticated financial crime.	The guidelines explain risk factors that need to be assessed. Following the risk-based approach, appropriate CDD measures should be applied. In this context, firms should take into account information from a variety of sources (see guidelines 1.29 to 1.31). Furthermore, for example, guideline 2.8 requires that firms should take into account FATF's typologies on TF.	*None*
Guideline 2	One respondent reflected that the ability to use ATMs should be included as a risk factor.	The involvement of an ATM is covered under Guideline 2.19.	*None*
Guideline 2	One respondent reflected that it was essential to stress that one factor itself might not be sufficient to imply a higher risk.	This principle is already reflected in Guideline 3.3 stating that firms should note that, unless Directive (EU) 2015/849 or national legislation states otherwise, the presence of isolated risk factors does not necessarily move a relationship into a higher or lower risk category.	*None*
Guidelines 2.3 and 2.7	Several respondents proposed to differentiate the identification of the risk factor associated with the customer from the identification of the risk factor associated with the beneficial owner, as the latter is not the customer of the firms.	Guideline 2.1 requires firms to identify risk factors relating to their customers, countries or geographical areas, products and services, and delivery channels. Guidelines 2.3 to 2.7 contain requirements on how to identify risk factors associated to the customer and the beneficial owner. The measures taken to understand who they are and to assess the ML/TF risk associated to them, are broadly the same.	*None*
Guideline 2.7	One respondent reflected that the list was not regularly updated and might imply that financial institutions concentrate on these characteristics, requesting a more flexible approach. One respondent suggested distributing these risk factors within the risk factors described in preceding guidelines. One respondent suggested that listing TF risk factors separately may have the unintended consequence of firms interpreting this as requiring them to assess them separate and apart from other customer risk factors. The same respondent also reflected that the wording of this Guideline could be misinterpreted to mean that terrorist financing risk should only be looked into where other high-risk indicators have been identified.	The EBA emphasizes that the non-exhaustive list of risk factors on terrorist financing was included following feedback of the industry during the public consultation of the first version of the Risk Factors Guidelines. Guideline 2.2 states that firms should note that the risk factors are not exhaustive, nor is there a requirement that firms will consider all risk factors in all cases. In the context of TF risk, it is expected that obliged entities take into account at least the risk factors provided in guideline 2.7. Firms need to take a holistic view, as mentioned in the guidelines.	*None*

Guideline 2.7 a)	Many respondents mentioned the difficulty of assessing whether the customer or beneficial owner are known to have close personal or professional links to persons registered on lists of persons, groups and entities involved in terrorist acts and subject to restrictive measures (for example, because they are in a relationship or otherwise live with such a person). One respondent states that the guideline could lead firms to investigate in all cases whether a potential customer had a close personal or professional link to a person designated and named on a 'sanction list', regardless of the level of possible TF risk present, compromising the risk-based approach. This respondent suggested an amendment to clarify the main sources of information that firms should use to verify these links. The same respondent also proposed to consider incorporating an additional paragraph clarifying (i) that in order to decide whether a person is known to have personal or professional links, the firm only needs to take into account any information which is in its possession, or which is publicly known, and (ii) that an active research by the firm is not required in the absence of other TF risk indicators. One respondent suggested to consider the criteria described in the OECD Handbook Money Laundering and Terrorist Financing Awareness Handbook for Tax Examiners and Tax Auditor, which describes on pages 70 to 79 the risk indicators related to TF, which may be detected during tax audit activities.	Firms should take into account the information available to them, whereby Guideline 1.29-1.32 set out the different sources of information that firms are expected to consider. Guideline 2.7 a) refers to 'known' personal or professional links. The Guidelines are clear that the risk factors are not specific to terrorist financing, but could point to increased TF risk, in particular in situations where other TF risk factors are also present. As stated above, firms should take a holistic view when assessing the different risk factors. Guideline 2.8 refers to Guidelines 1.30 and 1.31 regarding various sources of information firms should take into account.	*None*
Guideline 2.7 b)	Several respondents proposed deleting 'under investigation'.	In the EBA's view, there is no need to delete the referred text. If the information is public, firms should take it into consideration.	*None*
Guideline 2.7 c)	Several respondents interpreted that according to this guideline any country that has experienced a terrorist attack should be automatically considered as a high risk country.	The EBA does not support such a conclusion.	*None*
Guideline 2.7 e)	One respondent requested further clarification on what 'unclear links' mean.	Guideline 2.7 e) requires firms to take into account whether the customer might misuse (different) non-profit organizations (with unclear links) to move large amounts of money in a short time. Those non-profit organizations might be a part of any kind of	*None*

		financing network with the only aim of transferring funds between local and/or international accounts with illicit purposes. The guideline already contains example for unclear links.	
Guideline 2.7 f)	One respondent asked the EBA for clarification (i) whether there is the need to carry out checks not only on customers / executors / legal representatives / beneficial owners, but also on the 'non-customer beneficiaries' regarding subjects not specifically identifiable in the terrorist lists and (ii) how to identify a beneficial owner who is not a customer.	Firms should take into account whether the customer transfers or intends to transfer funds to persons referred to in guidelines 2.7 a) and b), meaning transfers to persons included in lists of persons, groups and entities involved in terrorist acts and subject to restrictive measures, to persons who are publicly known to be under investigation for terrorist activity or has been convicted for terrorist activity, or to individuals known to have close personal or professional links to such persons. Consequently, firms need to focus on the beneficiary of the fund transfer.	*None*
Guideline 2.8	One respondent proposed including the reference to FATF typology reports concerning terrorism as a factor incorporated into the methodologies of both business-wide and individual risk assessments.	The EBA is of the view that those typologies are already covered by Guideline 1.30 d) and e).	*None*
Guideline 2.9 c)	One respondent reflected that identifying the relevant financial or legal interest of retail customers or beneficial owners in other countries to determine risk level could potentially be excessive.	Guideline 2.9 c) does not require that firms carry out exhaustive assessments in all cases, but to take into account any information where the customer or the beneficial owner has relevant interests in a certain jurisdiction. In many cases, such information might have been already gathered by the firm in the on-boarding process.	*None*
Guideline 2.9 a) and 2.9 c)	One respondent reflected that the term 'resident' in guideline 2.9 a) was intended to include the tax residence of a customer or beneficial owner. Equally, the amendment in guideline 2.9 c), which refers to 'financial or legal interests' could also include the tax residence of a customer or beneficial owner.	The term 'resident' is defined in Article 1 j) of Regulation (EU) No 883/2004 on the coordination of social security systems as 'the place where a person habitually resides'. The Court of Justice clarified that the Member State of 'residence' is 'the State in which the persons concerned habitually reside and where the habitual centre of their interests is to be found.' It added that, '[i]n that context, account should be taken in particular of the employed person's family situation; the reasons which have led him to move; the length and continuity of his residence; the fact (where this is the case) that he is in stable employment; and his intention as it appears from all the circumstances'. The habitual centre of interests must be determined on the basis of the facts, having regard to all circumstances which point to a person's real	*None*

		choice of a country as his or her State of residence. Therefore, the term 'residence' already captures the concept of 'tax residency'. Equally the term 'jurisdiction' used in guideline 2.9 c) covers the place where tax residence is.	
Guideline 2.9 c)	Many respondents requested further guidance on the definition of 'business links, or financial or legal interests'.	The Risk Factors Guidelines require firms to assess several 'links', for example, the customer or the beneficial owner might have (see guideline 2.4, 2.7, 3.5, 4.57 and sectoral guidelines). The amended guideline 2.9 c) states that, when assessing the country or geographical risk, firms should also take into account any business links, legal or financial interests, the customer or beneficial owner might have in the context of jurisdictions. On business links, firms should, for example, assess whether the customer or beneficial owner performs any professional or commercial activities in the jurisdiction. On financial interests, firm should, for example, assess whether the customer or beneficial owner has any revenue, expenditure or asset in the jurisdiction (source of wealth and the source of funds). Other examples could include shares, other ownership rights and memberships. On legal interests, firm should, for example, assess whether the customer or beneficial owner has any legally enforceable rights.	*None*
Guideline 2.10 c)	One respondent argued that whilst in some parts of the overall Guidelines, reference is made to its requirements applying in relation to 'third countries', Guideline 2.10 c) does not limit consideration to these jurisdictions, and therefore proposes to add further clarification.	Firms should inter alia assess the ML/TF risk associated to countries. In case, there is a jurisdiction associated with higher ML/TF risk, firms should apply appropriate EDD measures. For completeness, as required by Article 18a of AMLD, firms should apply specific EDD measures in cases of 'high risk third countries'.	None
Guideline 2.10 d)	Several respondents required clarification, indicating that rather than referring to situations where a customer is 'a trust or any other type of legal arrangement', or 'has a structure or functions similar to trusts', the guideline should refer to 'legal arrangement that has a structure or functions similar to trusts'.	The guideline requires that, where the customer is a trust or any other type of legal arrangement, or has a structure or functions similar to trusts such as, fiducie, fideicomiso, Treuhand, firms should take into account the extent to which the country in which the customer and, where applicable, the beneficial owner are registered effectively complies with international tax transparency and information sharing standards. From a risk	*None*

		perspective, firms need to consider all types of 'arrangements', and should examine whether there is limited transparency in the context of such arrangements.	
Guideline 2.11 b)	One respondent mentioned that local obstacles to the application of group-wide policies and procedures should only be assessed when the group plans to set up a branch or subsidiary in a foreign country. One respondent reflected that the Commission delegated Regulation (EU) 2019/758 applies only to foreign countries where a firm's branch or subsidiary is established, and therefore the risk factor cannot be required for countries where a firm has no presence. Several respondents highlighted that the text of footnote 15 is missing.	Guideline 2.11 b) requires firms, when assessing the effectiveness of a relevant jurisdiction's AML/CFT regime, to take into account whether the country's law prohibit the implementation of group-wide policies and procedures and in particular whether there are any situations in which the Commission delegated Regulation (EU) 2019/758 should be applied. This regulation is of relevance for each third country where credit institutions and financial institutions have established a branch or they are a majority owner of a subsidiary. Also in cases where firms are planning to establish a branch or subsidiary in a third country, the EBA expects the firm to examine whether the country's law prohibit the implementation of group-wide policies and procedures. Having assessed the consultation responses on the missing text to footnote 15, the EBA has removed the footnote itself as there is no need for any reference.	*Footnote 15 has been removed*
Guideline 2.21	One respondent suggested including support to the use of financial technology in line with FATF recommendations, and requested more precisions as to how to mitigate potential residual risks of such situations.	The AMLD and the Risk Factors Guidelines are technology neutral. The guidelines include a section on CDD in non-face-to-face situations, including in situations where innovative CDD solutions are being used (see Guidelines 4.29 to 4.37).	*None*
Guideline 2.21.a) i)	Several respondents requested the EBA to provide further clarification for situations where there is no face-to-face contact with customers. They also queried whether the risk and mitigation is not already covered by the other articles of Guideline 2.21. One respondent asked whether there are always higher ML/TF risks associated with non-face to face business relationships or occasional transactions which would need to lead to EDD measures. One respondent suggested moving this letter to guideline 9 because the term 'customer' implied that this provision mainly	Guideline 2.20 requires that firms should consider the risk related to the extent to which the business relationship is conducted on a non-face-to-face basis. Guideline 2.21 states that firms should consider a number of risk factors, including whether the customer is physically present for identification purposes. If the customer is not physically present, Guideline 2.21 sub a) sub i) required the firm to assess whether there is a risk that the customer may have sought to avoid face-to-face contact deliberately for reasons other than convenience or incapacity. Having assessed the consultation responses, the EBA agrees that sub i) can be removed, as the key risk and its mitigation are already captured sufficiently by sub ii) and sub iii) that require the firm to consider	*'2.21 ~~a) i) […] considered whether there is a risk that the customer may have sought to avoid face-to-face contact deliberately for reasons, other than convenience or incapacity~~*

	addresses situations in a business relationship with natural persons and considered this provision contradicting to the content of Guidelines 4.29 to 4.31.	whether the firm used a reliable form of non-face-to-face CDD and has taken steps to prevent impersonation or identity fraud. The EBA has simplified guideline 2.21 a) accordingly, which may also reduce the administrative or reporting efforts that firms may have undertaken to comply with Guideline 2.21 sub a) sub i). Furthermore, the EBA notes that Guideline 2.21 a) refers to guidelines 4.29 to 4.31 whereupon, inter alia, firms should assess whether the non-face to face nature of the relationship or occasional transaction gives rise to increased ML/TF risk and if so, adjust their CDD measures accordingly. The EBA stresses that there are not always higher ML/TF risks associated with non-face to face business relationships or occasional transactions which would lead to EDD measures. The term customer contains any kind of clients that firms may have, including legal persons and other arrangements. The European Commission recently invited the EBA to draft guidelines, in 2021, on elements related to customer remote on-boarding and reliance on customer due diligence processes carried out by third parties. The EBA will publish draft requirements for public consultation in due course.	
Guideline 2.21 c) iii)	One respondent interpreted that the last sentence did not include third countries identified by firms as low risk with regulations applicable no less robust than in the EU.	The respondent's point relates to jurisdictions associated with lower ML/TF risk. To the contrary, guideline 2.21 c) iii) refers jurisdictions associated with higher ML/TF risk and high-risk third countries. With regards to third party reliance, firms should refer to Articles 25 to 29 of AMLD and guideline 2.21 c).	*None*
Guideline 2.21 c) iv) d)	Many respondents considered it would be difficult for the firm to satisfy itself that the level of CDD applied by the third party was commensurate to the ML/TF risk associated with the business relationship, interpreting that this requirement went further than the AMLD.	Firms are ultimately responsible for complying with their CDD obligations. This is why they should assess whether CDD obtained as part of a third party reliance arrangements is sufficient to meet their own CDD needs.	*None*
Guideline 2.21. f)	One respondent requested examples of AML/CFT obligations covered by this provision, asked whether an outsourcing service provider could be considered as an obliged entity if it is not	Firms should be aware of the difference between outsourcing arrangements and third party reliance (see Articles 25 to 29 of the AMLD, see guideline 4.34). In both cases, the ultimate	*None*

	regulated by EU law but by a third country AML law; and asked about the kind of interconnection with Guideline 4.34.	responsibility for meeting the relevant legal obligations remains with the firm. To the extent permitted by national legislation, firm may use an outsourcing service provider for any AML/CFT obligations. Firms should consider whether they have considered whether the outsourcing service provider is an obliged entity. Differentiation should be made between obliged entities under the AMLD and those regulated by third country law. Firms should also consider whether it has addressed the risks set out in the EBA's Guidelines on outsourcing (EBA/GL/2019/02), where those Guidelines are applicable.	
Summary of responses out of scope	1.) With regards to guideline 2.2, one respondent suggested adding at the end of this guideline: 'Firms may include others if relevant'. 2.) With regards to guideline 2.3, one respondent proposed adding a new letter 'd) The ownership and/or control structure of the customer (only applicable for legal entities)'. 3.) With regards to guidelines 2.3 to 2.9, several respondents interpreted the guidelines in a way that a risk assessment should also be done on the beneficial owners, which goes further than Article 8 of AMLD. One respondent also suggested deleting the word 'risk' to create a difference between risk factor and factor. 4.) With regards to guidelines 2.4 e) and f), 2.5 a), b) and c) as well as 2.6 c), e), f), j), k) and l), several respondents queried a number of specific expectations and/or provided concrete drafting suggestions. 5.) With regards to guideline 2.10, several respondents raised their concerns about the difficulty of knowing where their clients would generate funds. One respondent also requested further clarification. 6.) With regards to guideline 2.11 c), several respondents interpreted that the Guidelines assume an equivalence between the FATF itself and its regional bodies.	The suggestion is not related to any of the revisions to the guidelines that was proposed in the CP and therefore out of scope of the consultation.	*None*

	7.) With regards to guideline 2.14, several respondents queried the need and the drafting of the expectation and provided drafting suggestions. 8.) With regards to guideline 2.17, one respondent proposed deleting last part of the paragraph. One respondent requested examples of what kind of scenarios are meant. 9.) With regards to guideline 2.18 b), one respondent requested examples of what 'accept overpayments' meant. 10.) With regards to guideline 2.21 d) and e), one respondent requested clarification on what 'tied agents' and 'independent agents' mean.		
Feedback on responses to Question 4 (CDD measures)			
Guideline 4, general comment	One respondent asked the EBA to consider the adoption of a proportional approach regarding beneficial ownership, monitoring, and the CDD policy and procedures to be applied to credit unions, due to their cooperative structure, their not-for-profit tax status, and the benefits they provide their members as well as the benefits they provide to society.	Guidelines cannot alter the scope of application of obligations directly deriving from the AMLD. The EBA notes that art 8.1 of Directive (EU) 2018/843 and Guideline 1.16 explicitly take proportionality into account, stating that the steps firms should take to identify and assess ML/TF risk shall be proportionate to the nature and size of the obliged entities. Other factors mentioned by the respondents, such as the benefits credit unions provide to their members and to society are not relevant risk mitigating factors for AML/CFT purposes.	*None*
Guideline 4, general comment	One respondent generally advised to highlight throughout the guidelines the importance of the use of the Legal Entity Identifiers (LEIs) for a standardized, consistent and unique identification for legal entities as part of the CDD. Moreover, the respondent asked to Include an explicit recommendation by the EBA to the financial institutions that the Global LEI System should be used as the first step in identity verification and validation of legal entities as a trusted source.	The EBA refers to the analysis regarding the possible use of LEIs made above under 'general comments', not related to a consultation question.	*None*
Guideline 4, general comment	One respondent suggested to add further granularity and explanation on the extended data points that exist such as IP-address, Geolocation and Device ID. In addition, the respondent requests further clarification on what constitutes high risk activity	The EBA believes that there are no obstacles to the use of data/tools such as IP-Address, Geolocation and Device ID for CDD purposes. Moreover, for example the risk-factor in guideline 11.11 a) includes a reference to the IP address. Generally, firms	*None*

	and high risk industries in context of CDD/EDD, since the focus is deemed still too large on country-based risk, which has been not the most prevalent indicator of potential financial crime activity.	should assess the reliability and effectiveness of the different sources of information and to balance the usefulness of certain tools against the additional burden. As regards the second comment, the EBA considers that the Guidelines are sufficiently clear in requiring that firms follow a holistic approach, taking into account all relevant risk factors and weighing them against each other. Therefore geographical risks should not per se constitute high risk activity, unless Article 18a is applicable (guidelines 4.53 to 4.57).	
Guideline 4.7, 4.7 a) and 4.7 b)	Most of respondents that commented on Guideline 4.7 (a) underlined that beneficial ownership may not be ex ante defined in policies and procedures by category of products and services. As a consequence, it has been suggested to remove this reference to products and services from the text. Some respondents state that firms are according to guideline 4.7 supposed to clearly define at what point a series of one-off transactions amount to a business relationship. It would be beneficial according to the respondent if the competent authorities have the same rules and reference to Articles 5, 6 and 7 of the Wire Transfer Regulation (EU) 2015/847 would be made.	A beneficial owner may also be identified for a category of products, for instance where those products are intrinsically designed to be conducted on behalf of a natural person different from the customer (e.g. saving accounts for minors). In any case, the guideline already requires the identification of beneficial owner only 'where applicable'. Firms should indeed decide at what point a series of one-off transactions amount to a business relationship. This task is intentionally left to firms who know their business and their customer base and may rely on any indicative criteria to detect connections between one-off transactions that suggest the existence of a business relationship. Cross reference to Wire Transfer Regulation would not be conclusive in this sense and is in any case already included in article 11 of the AMLD. Finally, the EBA acknowledges that the last sentence of GL 4.7 letter a), i.e. "*what constitutes an occasional transaction in the context of their business*" is out of place and should be moved to letter b).	*4.7 a) [..] Firms should refer to the sectoral guidance in Title II of these guidelines, which has further detail on the identification of customers and their beneficial owners; ~~what constitutes an occasional transaction in the context of their business.~~* *b) Firms should clearly define <u>what constitutes an occasional transaction in the context of their business and</u> at what point a series of one-off transactions amount to a business relationship, rather than an occasional transaction, taking into consideration factors such as the frequency or regularity with which the customer returns for occasional transactions, and the extent to which the relationship is expected to have, or appears to have, an element of duration. [..]*

Guideline 4.9 to 4.10	Referring to Guideline 4.9, some respondents would welcome clearer guidance on how to reach a suitable balance between the competing aims of financial inclusion and financial crime prevention. Although to these respondents the rationale of the guideline is clear, many respondents deemed it very difficult to apply it, with some respondent asking for the deletion of guideline 4.9 altogether. With regard to guideline 4.10, one respondent asked for additional clarification and guidance from local authorities of which types of ID should be acceptable for which level of service. According to another respondent, exceptions listed in guideline 4.10 should only be applicable to private individuals and only in exceptional cases. One respondent asked for more proportionality with regard to the recommendation under guideline 4.10, to offer 'only basic financial products and services, which restrict the ability of users to abuse these products and services for financial crime purposes' to customers who are unable (for legitimate and credible reasons) to provide traditional forms of identity documentation, in order to avoid unreasonable or unnecessary limits to customers' access to financial products and services. One respondent remarked that Guideline 4.10 was not coherent with Article 14(4) AMLD, where it provides that if a customer has legitimate and credible reasons for being unable to provide traditional forms of identity documentation, firms should consider mitigating ML/TF risk in other ways, including by offering only basic financial products.	The EBA is committed to financial inclusion. The application of risk sensitive measures should enable more individuals and businesses, especially low-income, unserved and underserved groups, to access and use regulated financial services, and should increase the effectiveness of the fight against ML/TF. During the consultation period of these Guidelines, the EBA issued a separate call for input on de-risking and received more than 300 responses. Once the EBA has assessed the responses, it may or may not decide that clarifications are appropriate for some of its other legal instruments. Similarly, EU law confers explicit rights to individuals, such as the right under Directive EU (PAD) to access a basic bank account. In this regard the EBA has recommended the Commission's in its response to the call for advice (see EBA/REP/2020/25) to assess the extent to which national law prevents the application of risk-based AML/CFT measures that would facilitate the opening of payment accounts with basic features in situations where ML/TF risks exist and to take steps to clarify the interaction between AML/CFT requirements and the right to open and use a payment account with basic features, for example by including in the PAD a mandate for EBA guidelines. Guideline 4.10 is clear that firms, when balancing the need for financial inclusion with the need to mitigate ML/TF risk, should put in place appropriate and risk-sensitive policies and procedures to ensure that their approach to applying CDD measures does not result in unduly denying legitimate customers access to financial services. To make this more explicit, the EBA has included an additional clarification in Guideline 4.9. This approach is fully in line with Article 14(4) AMLD and confirms that firms need to apply CDD measures and to mitigate ML/TF risk, including transaction monitoring, in order to, for example, detect unusual or suspicious transactions. In that context, Guideline 4.11 refers to the EBA's Opinion on the application of customer due diligence measures to customers who are asylum seekers from higher-risk third countries or territories where additional clarification, inter alia, on situations is provided where	*Financial inclusion and de-risking* *4.9 'De-risking' refers to a decision taken by firms to no longer offer services to some categories of customers associated with higher ML/TF risk. As the risk associated with individual business relationships will vary, even within one category, the application of a risk-based approach does not require firms to refuse, or terminate, business relationships with entire categories of customers that are considered to present higher ML/TF risk. Firms should carefully balance the need for financial inclusion with the need to mitigate ML/TF risk.*

		a customer has legitimate and credible reasons for being unable to provide traditional forms of identity documentation.	
Guideline 4.12 ff. and 4.20 (c)	With reference to beneficial ownership (Guideline 4.12 ff.), respondents asked to amend guideline 4.12 (d) such that firms should determine the extent of the application of steps (b) and (c) on a risk-sensitive basis and to add a reference to large corporates with complex structures where it is reasonable to conclude that there is no beneficial owner, rather than expending what these respondents consider to be excessive efforts on a fruitless search. With particular regard to beneficial ownership registers in Guideline 4.13, some respondents made a number of different but interrelated suggestions, including: i) to clarify that the information contained in the Beneficial Owner register (hereinafter 'the Register') is prevalent when there are doubts or inconsistencies with other information taken by the intermediary and these discrepancies cannot be resolved with other available tools; ii) to clarify that firms should be allowed to use the beneficial ownership registers as the only data source; (iii) which additional steps should be taken to identify and verify the beneficial owner(s), other than using information contained in beneficial ownership registers; (iv) on more input on how these registers are to be made more effective and reliable in line with the letter and spirit of the EU Directive and the FATF standards v) With regard to the identification of the customer's senior managing officials, one respondent asked to delete the requirement under guideline 4.20 (c) for firms to assess whether the reason given by the customer as to why the natural person who ultimately owns or controls the customer cannot be identified are plausible, since this requirement is not set forth in the Directive. Another respondent considers the provision under guideline 14.15 b) to be disproportionate and proposes to delete it.	As regards beneficial ownership, the EBA deems that the wording in Guideline 4.12 let d) is sufficiently clear about the risk-based approach. The AMLD does not foresee exemptions from the requirement to identify the beneficial owner but does set out alternative options that firms can apply in some cases. Please refer to Guideline 4.19 for further detail on this. With regard to the beneficial ownership register, the EBA points out that: Regarding point i) and ii): Article 30, para 8 of the AMLD and Guideline 4.13 make clear that firms should conduct risk sensitive analysis to identify beneficial owners and may not solely rely on information contained in beneficial ownership registers. As a consequence, when they identify a beneficial owner who is different from the person indicated in the register, such information should prevail. Regarding point iii) Article 13 AMLD sets out an obligation to take reasonable measures to understand the ownership and control of the customer. To this end, firms may rely on any other useful information source, e.g. information drawn from public registers, constitutional acts, statutes, financial statements, prospectuses or other documents subject to disclosure obligations, information coming from public authorities. Regarding point iv) questions about amending and improving national beneficial ownership registers are not within the scope of these Guidelines. Regarding point v) Article 13, para 1, (b) of the AMLD and Guideline 4.14 provide that firms 'must take reasonable measures' to understand the customer's ownership and control structure. This means that, before identifying the customer's senior managers as beneficial owners, firms should assess the reasons why it was unable to identify any 'natural person who ultimately owns or controls the customer'.	*None*

	vi) One respondent felt there could be a possible confusion between the term 'plausible' (subjective) and the fact that all possible means for identifying the natural person should have been exhausted (objective).	Regarding point vi) Concerning the possible confusion between the terms 'plausible' and 'all possible means', respondents are reminded of Article 3(6)(a (iii) of AMLD5. As a consequence, the term 'plausible' should be interpreted as meaning that there are no grounds of suspicion.	
Guideline 4.14 and 4.16	One respondent underlines that the wording of the Guidelines 4.14 is not reflecting the whole definition of the beneficial owner, which includes any natural person (i) who ultimately owns or controls a legal entity, or (ii) on whose behalf a transaction or activity is being conducted, or (iii) who controls the legal entity by other means (e.g. *control structure*). Rather, so the respondent continues, the identification and verification of the beneficial owner implies to understand the customer's ownership and control structure. According to some respondents, Guideline 4.16 should be reworded so that is clear that if a suspicion arises due to the 'ownership and control structure', or the firm suspects that the funds are the proceeds of crime under Article 33(1) AMLD, then they should report to the FIU. As such, so the respondent continues, the 'and' in line two should be an 'or'. As regards suspicious reporting obligations some respondents suggested to amend Guideline 4.16, in order to require firms to report to the FIU suspicions arising from the customer's 'transactional activity or behaviour' and not from its 'ownership and control structure', as it is laid down in the consultation paper.	The EBA clarifies that the aim of guideline 4.14 is to explain that the requirement to understand the customer's ownership and control structure is part of the obligation to identify and verify the identity of the beneficial owner, as stated in article 13(b) of AMLD. As regards the suggested rewording of GL 4.16, the EBA points out that Article 33 of AMLD sets out a general obligation to promptly inform the FIU whenever it 'knows, suspects or has reasonable grounds to suspect that funds, regardless of the amount involved, are the proceeds of criminal activity or are related to terrorist financing' without specifying nor limiting the possible source of such suspicion. Guideline 4.16 clarifies that suspects may also arise from the customer's ownership and control structure. As a consequence, firms should inform the FIU whenever the customer's ownership structure is complex or opaque and this gives rise to suspicions that funds, regardless of the amount involved, are the proceeds of criminal activity or are related to terrorist financing.	*None*
Guideline 4.16, 4.67 and 4.73	One respondent asks to further clarify, with reference to guideline 4.73, the requirement that firms should review unusual and suspicious transactions and transaction patterns 'without undue delay'. Respondent ask for clarification whether it means after detection by tool, or after transaction took place.	As regards Guideline 4.73, the wording 'undue delay' relates to the point in time where the firm has become aware of the existence of a suspicion. It would be therefore inappropriate to establish a fixed timing.	*None*
Guideline 4.14, 4.12 and 4.20	Many respondents argue that in line with the AMLD firms should be required to take 'all reasonable steps' instead of 'all necessary steps' to verify the information provided by the customer to understand the customer's ownership and control structure and	The EBA agrees with the introduction of the 'reasonable measures' in line with Article 13(1)(b) of Directive (EU) 2018/843. The EBA therefore aligns the text of the Guidelines, more in particular 4.12 and 4.14 with the wording from Article 13 sub 1) b	*'4.12 c): Firms should then take all necessary and reasonable ~~steps~~ measures to verify the information: to*

	identify the natural person who ultimately owns or controls the customer.	of AMLD: 'Where the beneficial owner identified is the senior managing official as referred to in Article 3(6)(a) (ii), obliged entities shall take the necessary reasonable measures to verify the identity of the natural person.'	*achieve this, firms should consider using beneficial ownership registers where available.*' *'4.14: The requirement to identify, and take all necessary reasonable measures to verify the identity of, the beneficial owner relates only to the natural person who ultimately owns or controls the customer.'*
Guideline 4.17	Some respondents argued that the wording '*control through other me*ans' is too broad. Moreover, one respondent asks the EBA to clarify that control through other means will only be relevant if control through 'ownership' or 'control' of shareholdings cannot be established.	The concept of "control through other means" has been established in the 4th AML Directive. It should be interpreted broadly, and Guideline 4.17 aims at helping firms to interpret and apply it by giving examples of what "control through other means" can look like.	*None*
Guideline 4.19, 4.21 and 4.22	According to some respondents, guidelines 4.19 and 4.22 refer to new requirements identifying the beneficial owner and customer's senior managing officials. Guideline 4.19 is considered going beyond the requirement contained in Article 13 1) b) of the Directive. In many cases private companies do not have a beneficial owner through shareholding or control and their constitutional documents contradict the notion of designating the most senior official due to responsibilities over decision making being vested with the board of directors. Relatedly, one respondent asks the EBA to clarify whether this Guideline refers to the so-called 'fictitious beneficial owners'. If so, the respondent notes that the European supervisory authorities have issued different interpretations on whether all members of senior management must be identified as fictitious beneficial owners, or if it is sufficient to identify one member.	The provisions in Guidelines 4.19 and 4.22 explain what firms need to do to comply with the beneficial ownership requirements of a legal entity. If, after having exhausted all possible options and provided that there are no grounds for suspicion, no person has been identified, then the natural person who holds the position of senior management official should be identified as beneficial owner. On the second comment, Guideline 4.21 refers to the so-called fictitious beneficial owner. With regard to the question as to who has ultimate and overall responsibility/power to adopt binding decisions, the firm may be required to identify all members of senior management on a risk-based basis, depending on the customer's structure.	*None*
Guideline 4.20 b)	One respondent suggests supplementing guideline 4.20(b) with a clarification for the reader that, in case suspicion should arise, the	Article 14, paragraph 4 of the AMLD states that 'Member States shall require that, where an obliged entity is unable to comply with the customer due diligence requirements laid down in point	*None*

	firm should halt and potentially reconsider onboarding the customer.	(a), (b) or (c) of the first subparagraph of Article 13(1), it shall not carry out a transaction through a bank account, establish a business relationship or carry out the transaction, and shall terminate the business relationship and consider making a suspicious transaction report to the FIU in relation to the customer in accordance with Article 33.' The EBA deems this a legal obligation that does not have to be repeated in the Guidelines.	
Guideline 4.21	Several respondents stressed that the term of *senior managing official(s),* even if mentioned in the Directive EU 2015/849, is not clearly defined and remains subject to interpretation, which will in turn result in an ineffective application and enforcement. A comprehensive definition of this term, which is referred to several times in the whole Guidelines, would be welcomed.	Obliged entities should identify the customer's beneficial owner as defined in Article 3(6) AMLD. Guideline 4.20 further clarifies when and how to identify the customer's senior managing official(s) as beneficial owner(s). Guideline 4.21 requires that, when deciding which senior managing official(s) to identify as beneficial owner, firms should consider who has ultimate and overall responsibility for the customer and take binding decisions on the customer's behalf. The addition of a more specific definition of the term 'senior managing official' that is relevant in each case would not be feasible.	*None*
Guidelines 4.23 to 4.25	One of the respondents seeks for clarification how to identify the senior managing official for AML/CFT purposes in case the customer is a public administration or a state-owned enterprise. The respondent also asked whether or not a mayor or governor of region shall fall within the scope of 'senior managing official'. Some respondents argue that in guideline 4.25 the application of EDD should be based on the firms' risk assessment regarding the factors determining the PEP status. Respondents think that the mandatory EDD measures should only be applied when the senior management official of public administrations and state owned enterprises is a PEP in their own right and he/she is opening accounts as a private persons OR he/she is a senior managing officials, UBO or a legal owner of a private legal entity. The Joint Guidelines should confirm that so-called 'indirect PEPs', i.e. PEP sitting on the Board and acting as Director of a corporate or public or governmental body, are out of scope and should not be subject to EDD, except in situations where the PEP has full	For the identification of 'senior managing official' please see EBA analysis with regard to Guideline 4.21 above. The Guidelines explain how to identify the beneficial owner of public administration or state-owned firms. When such senior managing officials are PEP, firms must apply EDD measures to that senior managing official in line with Article 18 of Directive (EU) 2015/849, and assess whether the extent to which the PEP can influence the customer gives rise to increased ML/TF risk and whether applying EDD measures to the customer may be necessary. The Guidelines are clear that EDD is not needed in all cases where in respect of business relationships or occasional transactions with public administration or a state-owned enterprises in case a senior managing official is a PEP. The EBA, having assessed the consultation responses, believes that the first sentence of Guideline 4.25 should be amended, and has added 'of the customer' after senior managing official.	*'4.25: Firms should also have due regard to the possibility that the senior managing official <u>of the customer</u> may be a PEP.'*

	power to manage at his own discretion the corporate entity or the governmental body considered. Moreover, many respondents argued that it would be difficult or impossible for them to verify that the person they have identified as the beneficial owner is properly authorized by the customer to act on customer's behalf.		
Guideline 4.26	Several respondents considered the term 'remotely' in guideline 4.26 to be unclear as to its meaning.	Guideline 4.26 states that firms must verify their customer's identity and, where applicable, beneficial owners' identity, on the basis of reliable and independent information and data, whether this is obtained remotely, electronically or in documentary form. An example of a way to collect data remotely would be to use video-identification. Furthermore, the term 'remotely' is also used in other guidelines such as guideline 2.12 (e).	*None*
Guideline 4.27	One respondent asked to clarify what is a reliable and independent information/data and for more clarity on the use of adverse media and open source information like consumer advocacy websites, social media etc. The respondent asked for more consistency throughout the Guidelines by aligning the reference to reliable information/data around a common notion. In addition, the term 'degrees of reliability' in guideline 4.27 a) seemed unclear to some respondents.	The EBA believes that it is in line with the risk-based approach to ask firms to identify the information/data they will consider reliable and independent and by doing that, to assess the degree of reliability of such sources, information/data. To this purpose, the guideline give detailed guidance on which criteria might be useful, both to assess the reliability and the independence of information.	*None*
Guideline 4.28	One respondent asked to rephrase guideline 4.28 to clarify that, when assessing customer's and, where applicable, beneficial owners' identity, the 'quality of the evidence' provided by the customer can be a factor to be considered, but it does not represent a mandatory element of assessment. The respondent also asked for more proportionality when assessing the levels of independence and reliability of the sources (for example, for customers with very simple products or SDD, a less reliable source as evidence of certain elements should not necessarily impact negatively on the risk rating of such customer).	The requirement in guideline 4.28 is in line with the proportionality principle and the risk based approach, since it gives firms the responsibility to 'ensure that the method and type chosen is commensurate with the ML/TF risk associated with the customer.' Therefore, no changes are necessary.	*None*

Guideline 4.30	One respondent believes that guideline 4.30 as revised does not embed a risk-based approach. Respondent does not understand why a non-face-to-face activity should trigger enhanced due diligence. Respondent proposes that the guideline is revised to reflect that the key determinant for EDD is a high-risk interaction, not non-face-to-face activity.	The AMLD is clear that non-face-to-face business relationships or transactions, without certain safeguard, are indicative of potentially higher ML/TF risk and may require the application of EDD measures. The GL are consistent with the AMLD.	*None*
Guidelines 4.29 to 4.31	The Guidelines 4.29 to 4.31 refer to the application of customer due diligence measures in the context of non-face to face situations. Concerning such situation, one of the respondent asked for clarification on occasional transactions that could be conducted remotely.	Depending on the risk associated with a remote occasional transaction, firms should assess whether to put in place additional measures to be satisfied that they know who the customer is Guidelines 4.29 to 4.31 are applicable to occasional transactions.	*None*
Guideline 4.31	Some respondents asked to refer in guideline 4.31, not only to electronic means that provide a high level of assurance under Regulation (EU) 910/2014, but also to those that have been notified as electronic identification scheme in accordance to art. 9 of the same regulation; and to the use of an advanced electronic signature, based on a qualified certificate for electronic signatures, since qualified certificates can be issued only by Qualified Trust Service Providers (QTSPs) in accordance with article 24 of the same regulation.	The wording in guideline 4.31 already states the general principle according to which the use of electronic means of identification does not per se give rise to increased ML/TF risk. The reference to means which provide a high level of assurance is therefore not exhaustive.	*None*
Guideline 4.33	One respondent asked to expand the scope of guideline 4.33, so as to include a wider consideration of cyber risks, having in mind the variety of platforms through which the identification and verification means may operate. Moreover, the same respondent highlighted that more protection should be granted to employees against threats and other hostile consequence.	The EBA agrees with respondent that a potential cyber-attack that may affect the CDD innovative solution may create ML/TF risks. In this context, EBA has recently published its final Guidelines on ICT and security risk management which are addressed to PSPs, credit institutions and investment firms. Therefore, EBA replaces the reference to 'technical risks' with 'ICT and security risks' in order to refer to a defined and well-recognized term which also encompasses cyber risk. The measures firms take to protect their staff are outside the scope of these Guidelines.	*4.33. Firms that use or intend to use innovative technological means for identification and verification purposes [..].should have a clear view on:* *a) ~~technical~~ ICT and security risks, in particular the risk that the innovative solution may be unsuitable or unreliable or could be tampered with;*

Guideline 4.36	One respondent asked for confirmation that guideline 4.36 does not require firms to obtain prior approval from competent authorities regarding the use of a particular technology solution but rather requires them to demonstrate the appropriateness of the solution after implementation.	The EBA confirms that the interpretation of the respondent is correct, though national law or regulations can differ on this point. The language used in 4.36 is sufficiently clear to this purpose.	*None*
Guideline 4.38	As regards Guideline 4.38, on the elements which are part of the understanding of the nature and purpose of the business relationship, most of respondents underlined that the value and source of funds that will flowing through the account should only applied on a risk-based-approach basis, as per guideline 4.38 c). According to one respondent, the requirement set out in the Guideline 4.38 e) should only be executed when information sharing is allowed by law and group-wide policies. In addition, it should also only concern higher risk situations and international complex structures. Moreover, respondents claimed that the assessment of what would constitute a 'normal' behaviour, ref. 4.38 (f) could lead to various interpretations, and consequently could result in an ineffective enforcement/application.	The Guideline is clear that firms should understand the nature, value and sources of funds. There is no requirement that firms verify this in all cases. In general, information sharing always has to be in line with the legal requirements in force. The EBA considers it the firm´s responsibility to define what constitutes 'normal' or expected behaviour for this customer or category of customers, based on information gained during customer profiling, peer comparison or on the observation of past transactional behaviour, among other indicators.	*None*
Guideline 4.38	One respondent asked to amend guideline 4.38 (e) to clarify that, in accordance with the risk-based approach, only relevant customer information must be shared among companies that are part of the same group, such as higher-risk and FIU-reported customers/ parties, whereas the creation of a single database comprising all customers information would not be possible due to broad divergences among AML/CTF national laws.	Guideline 4.38 includes requirements on how firms should establish the nature and purpose of the business relationship in the context of the standard CDD measures. This obviously includes assessing whether the customer already has other business relationships with other parts of the firm or the group, and assessing how this affects the firm's understanding of the customer. The guideline does not prescribe how firms do such assessments.	*None*
Guideline 4.46	One respondent considers that guideline 4.46 does not take into appropriate consideration the fact that, following the adoption of EDD measures, the risks might be mitigated and shall therefore not be immediately considered 'high' anymore.	The EBA has decided to align the language of this provision with that used in article 18 AMLD.	*'4.46: AMLD lists specific cases that firms must always treat as high**er** risk.'*

Guideline 4.46	In Guideline 4.46, the scope of application of enhanced due diligence includes the business relationship or transactions involving high-risk third countries, in accordance with article 18 1) of AMLD. Most of respondents would be in favour of having the possibility to rely on a risk-based-approach and as such not applying an enhanced due diligence on all business relationship/transactions associated with high-risk third countries.	The need to apply enhanced due diligence measures to business relationship or transactions involving high-risk third countries stems from Article 18 of AMLD.	*None*
Guideline 4.48	Referring to guideline 4.48, one respondent asks the EBA to provide more clarification on how to adjust the list of functions in Article 3(9) of AMLD, with regard to prominent public functions from third countries. These may have materially different governmental and political structures in place e.g. level of prominence afforded to a 'Member of Parliament' in Europe is materially different to other countries?	Firms will have to determine who they should treat as a PEP based on their understanding of the institutional framework in the third country and the list of functions contained in the AMLD.	*None*
Guideline 4.49	One respondent requested clarity on the terms 'inconclusive' and 'not in line with the firm's expectations'. The respondent suggested completing the wording as follows: 'Firms that use commercially available PEP lists should ensure *on a best effort basis* that information on these lists is up-to-date and that they understand the limitations of those lists. Firms should take additional measures where necessary, for example, in situations *where they know that their automated screening framework and their screening results are inconclusive or not in line with their firm's expectations*.'	The aim of Guideline 4.49 is to stress that firms should not exclusively rely on commercially available PEP lists. The term 'senior management' is defined in Article 3 of AMLD through a reference to the officer or employee who occupies this function. It has the same meaning in these Guidelines. The aim of Guideline 4.49 is to create awareness on the limitations of commercially available PEP lists. An obliged entity must ensure at any time that the source of information is reliable, trustworthy and up-to-date.	*None*
Guideline 4.50	Guideline 4.50 sets out the measures which shall be taken by firms when identifying a customer or a beneficial owner who is a PEP. One of these measures require to obtain approval from senior management for entering into or continuing a business relationship with a PEP. This Guideline raises a broader question from the respondents on the term of '*senior manager*', which is not defined. For the sake of clarity, the respondents are in favour of having a clear definition of this term.	Article 3(12) AMLD provides a definition of the term 'senior management'. There is no need to limit the characteristics provided in this definition to a specific function.	*None*

Guideline 4.52	As regards PEPs, respondents asked i) to extend the recommendation in guideline 4.52 to ensure that the measures put in place in relation to PEPs do not lead to PEP customers being denied access to financial services, to all clients with high risk factors; and ii) to include a reference to de-risking at legislative level inserting the following 'Firms should ensure that the measures they put in place to comply with the AMLD and with these guidelines in respect of high risk factors do not result in entire categories of customers unduly being denied access to financial services.'	The EBA specifies that guideline 4.10, (b) already makes clear that firms should 'ensure that their approach to applying CDD measures does not result in unduly denying legitimate customers access to financial services'.	*None*
Guideline 4.53	One respondent asked the EBA to align its guidance with Article 18(1) of AMLD which deals with enhanced due diligence measures and high risk third countries. One respondent called on guideline 4.53 to be flexible enough to allow additional aspects to be considered in conjunction with the high-risk third country list when determining the level of EDD application. More generally, the respondent requested that the high-risk third country lists to be aligned globally to ensure consistency, and welcomes the European Commission's recent efforts in this respect.	The AMLD requires specific EDD measures to be applied to business relationships and transactions involving high-risk third countries as set out in Article 9(2) of AMLD. Consequently, guideline 4.53 refers to such business relationships and transactions where firms should ensure that they apply at a minimum, the EDD measures set out in Article 18a(1) and, where applicable, the measures set out in Article 18a(2) of AMLD. Having assessed the consultation responses, the EBA has made an editorial amendment in guideline 4.53 in order to align the requirement with Article 18a AMLD.	*'High-risk third countries* *4.53. ~~When entering into a~~ With respect to business relationships or transactions involving high-risk third countries as set out in Article 9(2) of Directive (EU) 2015/849, firms should ensure that they apply at a minimum, the EDD measures set out in Article 18a(1) and, where applicable, the measures set out in Article 18a(2) of Directive (EU) 2015/849.'*
Guideline 4.55, 4.56 and 4.57	Several respondents expressed the view that the definition of what should be considered as a business relationship or a transaction involving a high-risk country was too broad to be practicable. According to one respondent, it would be not manageable to consider that any single payment involving a high-risk third country should result in assessing the customer/transaction as high-risk and consequently in applying an enhanced due diligence on this business relationship/transaction. The respondent suggested changing the word 'transaction' to 'occasional	Article 18a AMLD with regards to business relationships or transactions involving high-risk third countries identified pursuant to Article 9(2) AMLD requires Member States to require obliged entities to apply specific EDD measures. The EBA, after having involved in particular the European Commission and national competent authorities, provides, in Guidelines 4.55 to 4.57, further clarification on what does 'involving high risk third countries' mean. The EBA included a list of key elements that all firms should assess at a minimum, whereby firms are free to also consider additional elements as they deem fit.	*'4.56 b) a customer's beneficial owner is ~~established~~ resident in a high risk third country.'* *'Guideline 4.57: Notwithstanding guidelines 4.54 and 4.56 firms should carefully assess the risk associated with business*

	transaction' to ensure that this requirement is triggered on a risk-based approach. For similar reasons, some respondents asked to delete Guideline 4.56. Firms might have limited knowledge of where the transaction passes through and there was no regulatory obligation to require collecting the address of the beneficial owner. One respondent asked the EBA to clearly set out what 'established in' a high-risk third country means. Many respondents requested to remove of Guideline 4.57 because firms might face difficulties to identify close personal links of a customer or a beneficial owner with a high-risk third country, and there was no official list available.	Article 18a AMLD refers, inter alia, to 'transactions' and not 'occasional transactions'. Having assessed the consultation responses, the EBA has made, for consistency reasons, an editorial amendment in guideline 4.56 b) in order to refer to beneficial owners being resident in high-risk third countries. Guideline 4.57 should be understood as an additional requirement to carefully assess the risk associated with business relationships and transactions where the obliged entity is aware of close personal or professional links with a high risk third country. Having assessed the consultation responses, the EBA has amended Guideline 4.57 to clarify that firms should take into account information available to them.	*relationships and transactions where* *a) the customer ~~maintains~~ is known to maintain close personal or professional links with a high-risk third country; or* *b) beneficial owner(s) ~~maintain(s)~~ is/are known to maintain close personal or professional links with a high-risk third country.* *c) In those situations, firms should take a risk-based decision on whether or not to apply the measures listed in Article 18a) of Directive (EU) 2015/849, EDD measures, or regular CDD measures.'*
Guideline 4.60 and 4.61	With regard to guideline 4.60 and 4.61, two respondents argue that in certain circumstances the enhanced due diligence applied may include enhanced monitoring however other forms of enhanced due diligence may be more appropriate.	Increased monitoring is mandatory (Article 18(2) AMLD). The guidelines provide additional clarification.	*None*
Guideline 4.64	Most of the respondents were not in favor of including the requirements of obtain information about family members and close business partners as part of the enhanced due diligence measures in cases where the family member or the business partner are not PEPs. Consequently, the respondents would prefer removing this language from the Guideline 4.64 or limiting its scope to the cases, when applicable. In addition, one respondent shared the view that the enhanced due diligence measures recommended under the Guideline 4.64 could raise concerns about or conflict with privacy rules and the	Guideline 4.63 sets out options for enhanced due diligence and is very explicit that firms are not expected to apply all enhanced due diligence measures listed in guideline 4.64 in all cases.	*None*

	storage of personal data, unless such measures are mandatory under the applicable AML/CFT laws in the relevant jurisdiction.		
Guideline 4.7, 4.72 and 4.74	As regards transaction monitoring, some respondents asked: - for more clarity under guideline 4.7 (f) on what the EBA means when mentioning the possibility that weaker forms of identification and verification of identity can be compensated by 'enhanced monitoring'; - to add the wording 'By having a written process in place to test the effectiveness of the transaction monitoring system' to guideline 4.72; - with regards to guideline 4.74, that requires firms to regularly perform ex-post reviews on a random sample taken from all processed transactions to identify trends that could inform their risk assessments, to add that these reviews should also be used to assess whether any transactions were missed, in order not only to improve the transaction monitoring system, but also to take action in case a transaction was overlooked); - also with regards to guideline 4.74, to consider that the quality of a transaction monitoring framework could be enhanced through information gathered from various external sources of information (such as FIUs, the FATF, Europol) that allow learning about the new typologies of ML/TF identified and help to define new scenarios or amending existing ones, and through regular tests on alerts generated and external triggers allowing the fine-tuning of the scenarios in place. This respondent mentioned not to see how tests on processed transactions could allow the identification of new trends and the enhancement of the reliability and appropriateness of the transaction monitoring system. Samples should not necessarily be random; - to explore the possibility of allowing disclosure of information (for the purposes of guideline 4.72-4.74) between two or more entities about a shared customer	The Guidelines allow obliged entities, in predetermined cases, to accept customers with fulfilling weaker upfront identification and verification (CDD measures) as necessary, if they ensure that an enhanced monitoring will compensate the initial CDD weakness. As regards the second comment, Guideline 4.72 requires firms to ensure their approach to transaction monitoring is effective and appropriate. Firms are asked to test the reliability and appropriateness of their transaction monitoring system, in Guideline 4.74, and their overall approach in terms of effectiveness, under Guideline 7. With regard to the third comment, Guideline 4.74 requires firms, in addition to real time and ex-post monitoring of individual transactions, and irrespective of the level of automation used, to regularly perform ex-post reviews on a random sample taken from all processed transactions to identify trends that could inform their risk assessments, and to test the reliability and appropriateness of their transaction monitoring system. Firms should consciously decide whether the sample should be chosen randomly in order to ensure a non-biased analysis. The guideline focuses on internal information (the sample of all processed transactions) that should be used to, as necessary, update, based on trends and developments regarding the behaviour of the customers, the risk assessments in particular of individual business relationships. The sample should also be used to assess whether the transaction monitoring system is reliable and, in particular, whether the respective indicators and alerts generated accordingly are appropriately calibrated. Guideline 4.74 is clear for firms to apply the risk-based approach when deciding on their transaction monitoring. In cases the sample tests reveal any transaction that is suspicious and has not already been reported, firms should report these transactions to FIUs following the usual procedures as soon as possible. The EBA	*'4.74 What is appropriate will depend on the nature, size and complexity of the firm's business, as well as the risk to which the firm is exposed. Firms should ~~refer to paragraphs [99(c) and 120 (c)])] [xxx] for guidance on~~ adjust~~ing~~ the intensity and frequency of monitoring in line with the risk-based approach. Firms should in any case determine […].'* *'4.75: In addition to real time and ex-post monitoring of individual transactions, and irrespective of the level of automation used, firms should regularly perform ex-post reviews on a ~~random~~ sample taken from all processed transactions to identify trends that could inform their risk assessments, and to test and, if necessary, subsequently improve the reliability and appropriateness of their transaction monitoring system. Firms should use the information obtained under Guidelines 1.29 to 1.30 also to test and improve their transaction monitoring system.'*

	or transaction (regardless of the professional category/sector) as long as those entities are under the same AML regime and subject to equivalent obligations as regards professional secrecy and personal data protection.	does not see a need to include this particular aspect in guideline 4.74. Equally, as mentioned in guidelines 1.29 to 1.31, to identify ML/TF risk, firms should refer to information from a variety of sources. Those information, for example on new typologies of ML/TF, should be used also for improving transaction monitoring systems. Having assessed the consultation responses, the EBA agrees that further clarification would be reasonable on external information and on the fact that a sample should not necessarily be random, and has amended guideline 4.74 accordingly. With regards to the last comment, sharing or disclosing information is out of scope for these Guidelines. Furthermore, the EBA has made an editorial amendment.	
Guideline 4.74	Many respondents argue that real-time monitoring should not be mandatory for Guideline 4.74 a).	Guideline 4.74 is clear that it will depend on the nature, size and complexity of the firm's business, as well as the risk to which the firm is exposed what is appropriate with regards to monitoring. The guideline requires firms to adjust the intensity and frequency of monitoring in line with the risk-based approach. They should determine which transactions they will monitor in real time, and which transactions they will monitor ex-post. As part of this, firms should determine which high-risk factors, or combination of high-risk factors, will always trigger real-time monitoring. Having assessed the consultation response, the EBA agrees that additional clarification would be reasonable, and has amended guideline 4.74 a) to the extent that it is expected that firms ensure that transactions associated with higher ML/TF risk are monitored in real time wherever relevant, in particular where the risk associated with the business relationship is already increased, emphasising the conscious decision to be taken by firms.	*'4.74* *a) Which transactions they will monitor in real time, and which transactions they will monitor ex-post. As part of this, firms should determine* *i) which high-risk factors, or combination of high-risk factors, will always trigger real-time monitoring; and* *ii) which ~~Firms should ensure that~~ transactions associated with higher ML/TF risk are monitored in real time ~~wherever possible~~, in particular those where the risk associated with the business relationship is already increased;*

Summary of responses out of scope	1.) With regards to guideline 4.41, several respondents requested additional clarifications on SDD measures. 2.) With regards to guideline 4.64, two respondents queried specific EDD measures. 3) With regards to guideline 4.67, one respondent asked to add to some wording.	The suggestion is not related to any of the revisions to the guidelines that was proposed in the CP and therefore out of scope of the consultation.	*None*
Feedback on responses to Question 5 (record keeping)			
Guideline 5.3. and general comment on applicability General Data Protection Regulation	Respondent suggests to include an additional paragraph in the Guidelines saying: '*In accordance to the AMLD, the collection, analysis, storage and sharing of data should be permitted, while fully respecting fundamental rights, for the activities required in the AMLD, such as, and not limited to, carrying out customer due diligence, ongoing monitoring, investigation and reporting of unusual and suspicious transactions, identification of the beneficial owner of a legal person or legal arrangement, identification of a politically exposed person, sharing of information by competent authorities and sharing of information by credit institutions and financial institutions and other obliged entities.*'	Article 43 of the AMLD establishes that the processing of personal data for AML/CFT purposes is a matter of public interest under the General Data Protection Regulation, while Article 41 mandates Member States to restrict data subjects' rights to access personal data where this right could interfere with the prohibition of disclosure in Article 39(1) of said Directive. The EBA acknowledges there may be some legal uncertainty associated with the processing of personal data in the AML/CFT context and therefore the EBA in its response to the European Commission's Call for Advice recently recommended that the Commission provide further clarity.	*None*
Guideline 5 and general comment on harmonization on record-keeping	Respondent calls on EBA to harmonize areas of EU law, including that on recordkeeping, to allow 'passporting' firms to comply with record keeping obligations in different jurisdictions and demonstrate to their competent authority that the measures taken are adequate. As an example, some EU countries require firms to keep documents for 10 years (Spain or Italy) and other EU countries only 5 years (France) after the relationship or professional service has ended, or the carrying out of the transaction. Respondent suggests that the EBA considers advising EU policy makers on a harmonized approach, in order to remove obstacles that impede the operation of the Single Market in payment services.	Record keeping requirements are set out in the AMLD and Member States have adopted divergent approaches to the transposition of the AMLD's record keeping requirements. This is the prerogative of Member States. Guideline 5 merely aims to clarify which information firms should at least record for their risk assessments. EBA notes that the remark is not related to the consultation question or revisions made to the guidelines.	*None*

Guideline 5, 1.4 and 1.6	Respondent refers to its comment on record-keeping under guideline 1.4 and asks EBA to provide more guidance regarding the recording requirement for risk assessments, so that firms can comply with a one set of rules, to effectively allow for more harmonization. Respondent furthermore welcomes further guidance on what records should be kept at a minimum (e.g. when a group-wide risk assessment should be considered sufficiently granular). Respondent suggests the wording previously used, namely: 'Firms must keep their risk assessment up to date and under review', provided more clarity and made clear credit institutions have an obligation to keep an audit trail and document the process.	As indicated above, the transposition of record keeping requirements is in the Member State derogative. Guideline 1.4 sets out that firms should record and document their business-wide risk assessment, as well as any changes made to this risk assessment in a way that makes it possible for the firm, and for competent authorities, to understand how it was conducted, and why it was conducted in a particular way. This guidance is deemed sufficiently detailed while respecting the legal framework. Where respondent comments on the need to keep risk assessments up to date: The revised guidelines still contain this criterion in Guideline 1.6.	*None*
Guideline 5.2	Respondent remarks in relation to guideline 5.2 that the threshold of being 'sufficient' is too vague and could leave room for too much differentiation and interpretation between the firms and local competent authorities.	Guideline 5.2 states that firms should ensure that the records they hold (are) sufficient to demonstrate to their competent authority that the measures taken are adequate in view of the ML/TF risk. The EBA believes this is in line with the risk-based approach and also respects the currently existing legal framework. As such, there are no grounds for additional requirements. At the same time, EBA notes that the verb 'are' was accidently omitted in Guideline 5.2 and this has been corrected accordingly.	*'5.2: Firms should ensure that these records <u>are</u> sufficient to demonstrate to their competent authority that the measures taken are adequate in view of the ML/TF risk.'*
Guideline 5.1 c)	Respondent suggests to restrict the documentation that credit institutions need to collect to a minimum. Guideline 5.1 c) requires credit institutions, for the purpose of Articles 8 and 40 of the AMLD, to keep records of transactions, whereby respondent suggests these should only be transactions outside of existing business relationships.	Article 40 AMLD requires obliged entities to record documents necessary to identify transactions, for a period of five years after the end of a business relationship with their customer or after the date of an occasional transaction. Hence the legal requirement covers both transactions in an existing relationship and occasional transactions.	*None*
Response out of scope	With regards to guideline 5.2, one respondent suggests more guidance could be given about the accessibility of the documents or record keeping duration which may or may not be subject to General Data Protection Regulation considerations.	The suggestion is not related to any of the revisions to the guidelines that was proposed in the CP and therefore out of scope of the consultation.	*None*

Feedback on responses to Question 6 (Training)			
Guideline 6.2	Several respondents suggested to expand the scope of training to also cover suspicious or unusual behavior.	The EBA agrees with the proposal to better align it with the legal text in the AMLD.	*'6.2. [..] firms should take steps to ensure that staff understand [..] c) How to recognise suspicious or unusual transactions and activities, and how to proceed in such cases.'*
Guideline 6.3	Respondent welcomes the inclusion of Guideline 6 concerning training and stresses its importance, while indicating that firms should bear the costs, that the training should take place under working hours and that employees are given enough resources to carry out their tasks. The respondent is concerned that, where national law requires certifications, this may not be efficient. Moreover, respondent suggests that the training guideline should also cover the relevant data protection requirements.	Article 46(1) of AMLD requires Member States to require that obliged entities take measures to make employees aware of the provisions adopted pursuant to this Directive, which include relevant data protection provisions and those measures shall include participation of their employees in special ongoing training programs. It does not specify the need for certificated and any such requirement is the prerogative of national legislators.	*None*
Guideline 6.3	According to the Guideline 6.3, firms should ensure that AML/CTF training is *'tailored to staff and their specific roles'*. Several respondents have asked for more guidance how to implement this in practice (e.g. whether an online based training module would be sufficient or how to organize this in big firms).	It is up to each firm to decide how to ensure that the training is tailored to the business responsibilities and ML/TF risks relevant to their staff members, e.g. whether that is done in a virtual or physical format.	*None*
Feedback on responses to Question 7 (reviewing effectiveness)			
General comment related to Guideline 7 on effectiveness	One respondent invites EBA to consider the effectiveness of the EBA guidance on combatting ML/TF, informed by the supranational risk assessment both when drafting this guidance and on an ongoing basis, whereby respondent argues that compliance with AMLD and the guideline will not effectively and efficiently combat ML/TF.	The EBA regularly reviews its guidelines and makes changes as necessary, including the Risk Factors Guidelines. Specifically, when updating these Guidelines, the EBA took into account new and emerging risks, including but not limited to those identified by the SNRA and the ESAs biennial Opinion and ML/TF risk, and findings from the EBA's AML/CFT implementation reviews report. Please refer to the background section of the report for	*None*

	Firms cannot meaningfully assess 'effectiveness' unless there is a feedback loop from regulatory authorities and law enforcement on the performance of the regime.	further details on this point.	
Guideline 7	Several respondents suggested the effectiveness review should be part of the risk assessment of a firm in order to have a coherent and sustainable risk-based approach. In addition, one respondent argued that an independent review of the effectiveness of a risk assessment approach should subsequently be done by a statutory auditor and that the guideline should refrain from recommending independent reviews by third parties which are not statutory auditors.	EBA notes that it does not see a need to require the effectiveness review to be part of the risk assessment, as the two assessments have a different scope and may have a different frequency. The Guidelines also do not prescribe how the review should be performed, nor by whom and leaves it to firms to decide on a risk-based approach.	*None*
Guideline 7.2	Guideline 7.2 states that 'firms should consider whether an independent review of their approach may be warranted or required'. One respondent asks what is meant by 'independent review' in the context of this guideline, on what basis it is required and whether this is an internal or external review. A second respondent considers it helpful if there would be greater focus on the rationale for engaging an independent review, what type of review that would entail and the specificity of the requirement. A third respondent argues that there should be additional criteria for an effectiveness review to be required, for instance only if the second or third "line of defence" detect potential high-risk issues that directly impact the firm's risk profile. And that the independent review should focus only on specific AML controls (for example, enhanced due diligence process or transaction monitoring aspects), rather than the complete AML program. As well as being a more proportionate approach, this would also reduce the cost of implementation of this recommendation for firms, in the view of the respondent.	Firms need to consider all circumstances when deciding if there is a need to perform an independent effectiveness review and what it should look like. The review could take place on whole or part of its policies, processes and procedures and could be done internally or externally, whereby firms also need to take into account the (national) requirements applicable to them – in some Member States, an external review by a certain profession may be required. In any case, firms should be able to justify their approach to their competent authority. The limitations suggested by the respondent are deemed too restrictive and the EBA sees no need to set additional criteria.	*None*
Guideline 7.2	One respondent argues that some firms due to their nature, size and complexity may not require an independent review of their approach. This should be included in the guideline.	The Guidelines are already clear that firms need to consider the relevant circumstances. However, size is not necessarily a reliable indicator for the degree of risk. Past cases of AML/CFT failures have shown that money laundering and terrorist financing occurs also in small firms.	*None*

Guideline 7.2	Respondent stresses the need for the management board to remain fully responsible for defining the risk appetite, and that the AML processes and safeguards are drawn up in close cooperation with the regulator. Respondent calls on guideline 7.2. to be amended to clearly reflect article 8(4)(b) of AMLD which notes that an independent audit function is required in exceptional circumstances only depending on size and nature of the business in question. Moreover, respondent believes that obliged entities established in one market that rely on a passport to operate in another, should only be obliged under the rules of the home member state.	Guideline 7.2 does not change anything to the applicable legal responsibilities for the management board. Guideline 7.2 already links to Article 8 sub 4 sub b) so it is sufficiently clear that firms where appropriate with regard to the size and nature of the business, need to have an independent audit function to test the internal policies, controls and procedures. AMLD does not state however that an independent audit is only necessary in 'exceptional circumstances', as respondent suggests, as Article 8.4 b) clearly specifies that an independent audit should be carried out 'where appropriate' which is not equivalent to 'in exceptional circumstances'. The Risk Factors Guidelines do not contain any rules on pass-porting and the firm needs to make its own assessment which services it can provide under which license and under what conditions.	*None*
Guideline 7.2	One respondent argues that EBA guidance should be directed where possible at improved information sharing between Financial Intelligence Units, law enforcement and the private sector as a means of measuring effectiveness. In the longer term, legislative action will be required to fully integrate information sharing credit institution-to-credit institution, government-to-credit institution, and enterprise wide for financial institutions. However, incorporating an expectation of increased information sharing as a means of measuring effectiveness in AML/CFT compliance would be a beneficial step for the final guidelines.	It is up to the firm to regularly assess the effectiveness of its approach and to decide how it wants to do so, including which measuring metrics it wants to use. The Risk Factors Guidelines do not prescribe any metrics on how to measure effectiveness and the EBA stresses that firms need to do what is legally required and in line with the risk-based approach.	*None*
Guideline 7.2	One respondent stressed the role that FIUs can play in developing effective AML/CTF programs, including having a clear understanding of the risks; assessing controls against the identified risks; using a risk based approach to prioritise resources; engaging actively with law enforcement; and, using both quantitative and qualitative factors to demonstrate the effectiveness of the programme.	Guideline 1.31 states that firms should take as input the information from FIUs, amongst information from a variety of other sources. As such firms cannot solely rely on FIUs, and FIUs are also not directly addressed by the Risk Factors Guidelines.	*None*

Summary of responses out of scope	1.) With regards to guideline 7.1, one respondent considers the assessment of effectiveness to be subjective. Several respondents requested further clarifications. One respondent mentioned that effectiveness is a core topic for driving a true risk-based and proportionate AML/CTF regime. 2.) With regards to guideline 7.2, one respondent mentioned that there is scope to ensure the concomitant effectiveness of communication between regulated entities and authorities in order to increase effectiveness.	The suggestion is not related to any of the revisions to the guidelines that was proposed in the CP and therefore out of scope of the consultation.	*None*
Feedback on responses to Question 8 (correspondent banks)			
General comment provided under Question 8	One respondent invited the EBA to consider issuing guidelines on Sovereign Bonds or Sovereign borrowers from highly corrupt countries.	Firstly, the EBA points out that the comment refers to a part of the Guidelines that was not amended and is therefore not under consultation. Secondly, the EBA does not consider to propose any new guidelines at this point in time due to the nature of the consultation. Thirdly the rationale for such guideline does not become sufficiently clear from respondent's comments.	*None*
General comment relating to guideline 8	Some respondents asked to clarify that for natural persons 'established in' should be interpreted as 'being resident', and for financial firms 'established' should be considered as 'the country where the respondent has its principal regulatory authority'	The EBA agrees that 'natural persons that are established in' should be interpreted as 'natural persons being resident in'. The EBA considers that the general criterion for identifying the country where legal persons are based is the country where they have their head office (see article 2, (f) or article 45, para 9 of AMLD). Therefore, the EBA considers the second suggestion by respondent not valid and no further changes are needed.	*None*
General comment relating to guideline 8	One respondent asked to clarify whether the requirements set out in Guideline 8 shall also be subject to the annual review under guideline 1.7.	The EBA confirms that the firm's business-wide risk assessment should include also the firm's correspondent banking activity.	*None*
General comment	Some respondents asked whether the scope of Guideline 8 covers also other correspondent relationships (pursuant to the definition referred to in article 3 sub 8 of the AMLD), in particular those	GL 8.1 is clear that, although specifically directed at correspondent banks, this guidance is also relevant for other correspondent relationships.	*None*

relating to guideline 8	amongst financial institutions for the purposes of securities transactions.		
General comment relating to guideline 8	One respondent invited the EBA to consider encouraging correspondent banks to consistently use the LEI for respondent bank identification to enhance its CDD and AML/CFT capacities. Regardless of the type of CDD performed (whether ordinary, enhanced or simplified), EBA may consider to recommending financial institutions to obtain an LEI for each legal entity client, considering the benefits which could arise from it.	The EBA refers to the analysis regarding the possible use of LEIs made above concerning general comments not related to a consultation question.	*None*
Guideline 8.6	Under guideline 8.6 (g), EBA is requested to add, after the respondent´s failure to provide the information requested by the correspondent for CDD and enhanced due diligence purposes, also the failure to provide information requested for transaction monitoring purposes.	Article 13 of Directive (EU) 2015/849 is clear that the term CDD includes transaction monitoring and thus, requests for information for CDD purposes include information necessary for transaction monitoring purposes.	*None*
Guideline 8.10 and 8.17	Some respondents asked i) Clarification regarding the obligation, under guideline 8.17, (e), to conclude a written agreement in order to document the responsibilities of each institution and if the current practice of communicating specific restrictions or limitations to the relationship with the respondent bank via Swift message is allowed under the revised guideline. ii) to confirm that requirements under i) until iv) are intended only as non-exhaustive examples of what can be documented in the written agreement and that/if they only apply to newly established relationships. iii) To clarify what is meant by requesting the respondents to include, in the written agreement, indication of the way correspondent will monitor the relationship, to ascertain the respondent complies with its responsibilities (confidentiality obstacles).	With regard to the first point, the EBA notes that the guidelines do not specify the form the written agreement should take. Secondly, the EBA confirms that the requirements set up by guideline 8.17, sub e) i) until iv) are a minimum list. Firms may determine additional elements to be agreed in writing. As with other aspects of these Guidelines, firms should apply these provisions to all correspondent relationships. This may include taking risk-sensitive measures to update existing agreements. Thirdly, the EBA points out that guideline 8.17 e. iii) requires that the written agreements indicate how the correspondent intends to satisfy himself that the respondent complies with the terms of such agreement but it does not prescribe how correspondents should do that. It is thus the responsibility of each correspondent to identify the most appropriate way to comply with this guideline, considering also confidentiality. With regard to the fourth point, a request for information in case of missing information or in case of alerts can be part of the transaction monitoring process or it may be triggered by customer due diligence measures (both simplified and	*None*

	iv) Whether the requirements set out in iii) and iv) relate to the request for information process in relation to missing payer/payee information required in the Funds Transfer Regulations and to the request for information required to address alerts from transaction monitoring/screening; v) To clarify that the requirements under sub e) i) until e) iv) are required for new business relationships only.	enhanced). It is not limited to obtaining information to comply with the Wire Transfer Regulation. Lastly the EBA clarifies that, pursuant to article 14.5 Directive (EU) 2015/849, firms need to apply CDD measures also to existing customers on a risk sensitive basis and when a change in circumstances requires such update. The revised guidelines clearly state that risk assessment and mitigation is an ongoing process and that firms must make sure that any new controls apply to new customers as they apply to existing customers. As a consequence, the requirements under guideline 8.17 i) until iv) also apply to existing relationships, albeit on a risk-sensitive basis.	
Guideline 8.10 and 8.17	One respondent highlighted a possible inconsistency between guideline 8.10, where transaction monitoring is considered mandatory, and 8.17 e) iii), which refers to ex post transaction monitoring only as an example of how the correspondent may monitor the relationship to ascertain how the respondent (based in a non EEA country) complies with its responsibilities under the agreement.	The EBA considers that no inconsistency exists between guideline 8.10 and guideline 8.17. Guideline 8.10 states that post-execution monitoring is the norm, which means that this is the standard measure due to the nature of corresponding banking. Guideline 8.17 refers to 'ex post transaction monitoring' as one of the possible ways the correspondent might monitor the consistency of the respondent's behaviour with the corresponding agreement. At the same time, real time monitoring can be another effective way of monitoring transactions, as set out in guideline 8.25.	*None*
Guideline 8.12	One respondent invited the EBA to clarify that guideline 8 does not require any type of customer due diligence on the respondent's customers.	As stated in Guideline 8.12, correspondents are not required to apply customer due diligence measures on the respondent's individual customers.	*None*
Guideline 8.13	One respondent asked to clarify why, under Guideline 8.13, customer due diligence questionnaires provided by international organisations are not considered as being part of the CDD measures the correspondents could use to comply with their CDD obligations.	The EBA clarifies that Guideline 8.13 does not state that such questionnaires should not be used, but it asks firms to be mindful that such questionnaires are not normally specific to ensuring compliance with AMLD. This is why firms that use these questionnaires should assess whether they will be sufficient to allow them to comply with their obligations under Directive (EU) 2015/849 and to take additional steps where necessary.	*None*
Guideline 8.17	A few respondents considered the amendments under guideline 8.17 (a) too prescriptive and asked to amend the wording so as to refer only to the possibility of asking respondents about its	Firms are legally required to understand the nature of the respondent's business. Guideline 8.17 (a) sets out how firms can	*None*

	customer groups (e.g. retail customers, institutional customers) and not also about individual customers.	do this but leaves it to each firm to determine on a risk-sensitive basis the steps it will take to comply with this requirement.	
Guideline 8.25	In relation to Guideline 8.25 (b), one respondent asked the EBA to delete the reference to on-site visits, either conducted by the correspondent bank or by a third party. With regard to third party reviews, adding a third party review to the assessment of the AML/CFT framework performed by the third line of defence (internal audit) and by the supervisor, would create more burden on the teams.	The Guidelines list onsite visits and third party reviews as examples of measures firms may decide to take where the risk associated with the correspondent relationship is particularly increased. This is in line with international guidance and good practice. The guidelines do not require onsite visits or third party reviews as a matter of course.	*None*
Guideline 8.17	One respondent asked how firms should assess the quality of a country supervision under guideline 8.17 (b), in the absence of recent FATF reports on the relevant country.	Firm can determine the quality of a third country's supervision from publicly available resources. These are not limited to FATF reports. GL 2.11 also provides more information on this point.	*None*
Guideline 8.20	One respondent asked for more clarity on how a firm is expected to support financial inclusion through a proportionate and risk-based approach to enhanced due diligence measures and/or through supplementary risk-based enhanced due diligence measures, under guideline 8.20, in case it legitimately decides to establish a correspondent banking relationship with a respondent situated in a high risk third country by mitigating this risk.	EBA confirms that nothing in these guidelines prevents firms from establish a correspondent banking relationship with a respondent situated in a high risk third country, provided that the risk is mitigated through the enhanced due diligence measures s. In order for the firm to support financial inclusion, the EBA specifies in GL 4.10, (b) that firms should ensure that their approach to applying CDD measures does not result in unduly denying legitimate customers access to financial services. Therefore, policies and controls in place need to be commensurate to the risks identified.	*None*
Guideline 8.21	Respondent asked with regard to Guideline 8.21: i) to delete the requirement to determine the likelihood of the respondent initiating transactions involving high-risk third countries; ii) confirmation that identifying professional or personal links that the respondent's customers may have with certain countries is not considered a standard CDD measures, (considering the workload that this would imply and the risk that this could result in de-risking decisions) but rather as part of an enhanced assessment of a high-risk relationship; and	With regard to the first two points, the guidelines provide that firms have to take the steps necessary to understand the ML/TF risk associated with a correspondent relationship. This includes firms taking steps to understand the risk that the relationship exposes them to ML/TF risks associated with HRTCs and the firm taking risk sensitive measures to mitigate such risk. With regard to the third point, the EBA does not consider it necessary to define 'significant proportion' since firms need to take a risk-based approach considering both the likelihood and impact of such exposures.	*None*

	iii) for more detailed circumstances under which a 'significant proportion' is considered to be relevant, how the significance should be assessed and how firms are expected to collect relevant information on the respondent's customers having links with HRTCs.		
Guideline 8.23	One respondent asked to reconsider the approach under Guideline 8.23, aimed at applying in parallel the specific enhanced due diligence requirements for high risk third countries and the specific enhanced due diligence requirements for correspondent banking (assuming this interpretation of Guideline 8.23 is correct).	The EBA clarifies that Guideline 8.23 states that firms can meet their legal obligations under art. 18a (1) of the Directive (EU) 2015/849 by complying with the measures set out in articles 13 and 19. The specific requirements in art. 18a will be necessary only if the firm has assessed the risk as particularly high.	*None*
Guideline 8.24	Some respondents asked to reconsider the reference made in Guideline 8.24 to the need for correspondents to assess the adequacy of the respondent's policies to establish the source of wealth and source of funds of its clients: The determination of source of wealth and source of funds is only required for high risk clients, which may represent only a small percentage of respondent's customers. Furthermore, non-EEA respondents should not be subject to the same high risk third country measures which the EU correspondents should apply (except when FATF calls for counter measures to such jurisdiction).	This Guideline sets out how firms can comply with their obligation under Article 18a (1)(c) of the AMLD, which requires firms to obtain information on the source of funds and source of wealth of the customer and the beneficial owner(s).	*None*
Guideline 8.25	Regarding guideline 8.25 c), one respondent proposed to amend the text replacing 'should' with 'may', in order to guarantee that real time monitoring is applied by respondents only in specific situations and not as a compelling measure.	The Guidelines require firms to 'consider' real-time monitoring. It is up to each firm to decide, on a risk-sensitive basis, whether to apply real-time monitoring in those cases.	*None*
Summary of responses out of scope	1.) With regards to guidelines 8.5 a), 8.6 e) and 8.8 b), several respondents queried the risk factors. 2.) With regard to guideline 8.5 (a), how to interpret a relationship limited to a SWIFT (RMA) capability as a low risk factor and recital 43 of Directive (EU) 2015/849, stating that '*correspondent relationships do not include one-off transactions or the mere exchange of messaging capabilities*'.	The suggestion is not related to any of the revisions to the guidelines that was proposed in the CP and therefore out of scope of the consultation.	*None*

	3.) With regard to guideline 8.6 (e) to delete the reference to PEPs. 4.) With regard to guideline 8.8., further clarification on what is considered to be 'significant business' or how firms can assess whether the respondent is subject to non-effective AML/CFT supervision. 5.) With regards to guideline 8.10 b), one respondent asked whether the requirement to document the responsibilities of each institution in an EEA correspondent banking relationship would introduce further responsibilities than those envisaged by Article 19(d) of the AMLD which only require institutions to document their responsibilities in non-EEA cross-border correspondent banking relationships. 6.) With regards to guidelines 8.17 b) and 8.17 d), several respondents requested further clarifications. 7.) With regard to guideline 8.17 c), many respondents pointed out that the obligation for correspondents to perform on-site visits or sample testing to assess the correct implementation of policies and procedures by respondents is too burdensome. 8.) In general, that a correspondent bank is not required to carry out CDD on all of the members of a credit union, but only on the members of the board. Respondent asks for a reference to the Financial Action Task Force's 'Interpretive Note' to Reduce De-Risking in Correspondent Banking, in particular to note that for correspondent banks when dealing with credit unions the firm does not need to perform due diligence on all of the members of a credit union, but that CDD on just the board members will be sufficient for purposes of AML/CFT. The same respondent suggests to use the 'Request for Information' process that FATF has included in its Guidance on Correspondent Banking Services issued in 2016.		

Feedback on responses to Question 9 (retail banks)			
Guideline 9	One respondent mentioned that necessary steps should be highlighted to ensure high quality non-face-to-face identification. This respondent also stated that concern of money mules created from social engineered, stolen, faked identity were not reflected in the guideline and should be considered to be added in detail to the guideline.	Guidelines 4.29 to 4.31 provide guidance on non-face to face business relationships, which is also relevant to retail banks, while identity fraud is highlighted as a risk in Guideline 2. Guideline 9.6 contains references to unusual customer behaviours. The Guidelines are clear that the sectors-specific guidance should be read in conjunction with the general guidance of Title I that is applicable to all sectors.	*None*
Guideline 9	One respondent commented, that EU-licensed gambling businesses are subject to the European Union's Anti-Money Laundering Rules since the inclusion of the whole sector in the Fourth Anti-Money Laundering Directive in 2015. This was a move that the sector had strongly advocated for and consequently welcomed. The respondent argued that the mere fact that the customer is a gambling business does not mean that the business poses a higher risk.	Gambling as an activity is associated with higher ML/TF risk. The guidelines are clear that banks need to reflect that in their risk assessment of the customer. As with all risk factors, the Guidelines are clear that an isolated risk factor may not push the entire relationship into a higher or lower risk category, and firms should take a holistic view of all risk factors to determine the most appropriate approach to managing the risk they have identified.	*None*
Guideline 9.10 a)	Two respondents suggested to clarify the term 'electronic identification certificates'.	Having assessed the consultation responses, the EBA agrees with the concern and is of the view that the Guidelines should be in line with Article 3(2) of Regulation (EU) No 910/2014 (eIDAS Regulation) with regards to 'electronic identification means'. The EBA has therefore amended the guideline and for the sake of consistency, implemented similar changes in guidelines 10.8 a); 14.10 a) and 17.7 a).	*'9.10 a) non-face-to-face business relationships, where no adequate additional safeguards – for example electronic signatures, electronic identification ~~certificates~~ means ~~issued~~ in accordance with Regulation EU (No) 910/2014 and anti-impersonation fraud checks – are in place.'*
Guideline 9.20	One respondent suggested to add a reference to the definition of virtual currencies in AMLD. The scope of the term 'virtual currencies' should be clarified. One respondent raised that virtual currencies should be defined in the guidelines in order to clarify whether this intends to capture the entire scope of crypto-assets, or a smaller subset of crypto-	The guidelines use the definitions contained in in the AMLD, unless specified otherwise.	*None*

	assets that are used for payment and that are widely currently unregulated.		
Guideline 9.20	One respondent suggested that an ICO that exchanged utility/payment tokens for other virtual currencies (which was the most common form of an ICO) or a stable coin should also fall under AMLD definition of a virtual currency exchange. This respondent also explained additional suggestions regarding a future legal AML/CFT framework in the EU. This respondent also mentioned that retail banks were often discriminating against virtual currency businesses, as they blocked their customers when these tried to transact with Virtual Assets Services Providers.	The EBA is not in a position to change EU law. Equally, the EBA recently provided advice to the EC on a future EU AML/CFT framework (EBA/OP/2020/14 and EBA/REP/2020/25), recommending, inter alia, that the EC has regard to recent revisions to the FATF standards and guidance regarding 'virtual assets' and 'VASPs', and changes to the scope of EU AML/CFT legislation to bring activities that are not currently covered, such as crypto-to-crypto exchanges within the scope of the AMLD in line with the FATF's Recommendations and the FATF's evolving approach. Furthermore, the guidelines do not support discrimination against or the wholesale de-risking of any category of customers but instead provide firms with tools to manage ML/TF risk effectively and efficiently.	*None*
Guideline 9.20	One respondent questioned why the sectoral guidance for Virtual Currencies has been included in the sectoral guidance for retail banking. This respondent mentioned that the EBA should comment as to whether virtual currencies should be aligned with the funds transfer regulations.	Guidelines 9.20 to 9.23 provide requirements when a credit institutions enters into a business relationship with customers that provide services in relation to virtual currencies. The EBA recently provided advice to the European Commission (EC) (EBA/OP/2020/14 and EBA/REP/2020/25), inter alia on the application of Regulation (EU) 2015/847 to virtual asset service providers.	*None*
Guideline 9.21	One respondent requested clarification on the due diligences measures to be performed in order to assess risks linked to customers that provided services related to virtual currencies.	The EBA refers to guidelines 9.20 to 9.24 which set out how retail banks should manage, in line with Title I of the Risk Factors Guidelines, the risk associated with such customers.	*None*
Guideline 9.22	One respondent requested clarification on what was considered a virtual currency in the context of a 'virtual currency trading platform', 'custodian wallet services', or 'arranging, advising or benefiting from initial coin offerings. With regards to guideline 9.22 e), one respondent mentioned that ICOs were not limited to virtual currencies but included also security tokens for which specific due diligence had to be performed. They were also not limited to retail banking. The	The guidelines use the definitions contained in in the AMLD, unless specified otherwise. In this context, the EBA has amended, for consistency, guideline 9.22 a) that refers to virtual currencies. With regards to the second comment, the EBA notes that guideline 9.22 e) requires credit institutions to consider 'arranging, advising or benefiting from 'initial coin offerings' (ICOs)' as virtual currency businesses. The EBA does not see the need for additional guidelines. Guidelines 9.20 to 9.23 provide	*'9.22 a) Operating as a virtual currency trading platform that effects exchanges between fiat currency and ~~cryptocurrency~~ virtual currency.'*

	respondent suggested to delete this guideline and to create two new guidelines on security tokens and on ICOs.	requirements when a credit institutions enters into a business relationship with customers that provide services in relation to virtual currencies.	
Guideline 9.23	One respondent suggested to delete the blanket prohibition on simplified due diligence for virtual currency business customers that have been assessed to be low risk. Two respondents proposed that additional due diligence or adverse media checks should be required on senior management of virtual currency businesses only as part of risk-based enhanced due diligence. Further guidance and recommendations could also be directed towards virtual currency businesses on how they could support proportionate and effective risk assessment and CDD in relation to privacy-enhancing features.	Considering the ML/TF risk associated with virtual currencies as stated in Guideline 9.20, SDD is unlikely to be appropriate. The Guidelines 9.20 to 9.24 reasonably reflect the increased ML/TF risk.	*None*
Guideline 9.23 e)	One respondent requested clarification on how to assess whether a business was legitimate.	Firms should apply guideline 9.23 in line with guidance set out in Title I of the Risk Factors Guidelines, for example in Guideline 4. The guidelines provide several approaches how to assess whether the business is legitimate.	*None*
Summary of responses out of scope	1.) With regards to Guideline 9.6 and 9.8, two respondents queried particular risk factors. 2.) With regards to Guideline 9.10 a), two respondents suggested to amend the requirements regarding 'electronic signatures'. 3.) With regards to Guideline 9.10 b), one respondent suggested that reliance on third party's CDD measures should be independent of the duration of the relationship between the firm and the third party. One respondent considered a reliance on a third party not contributing to increased risk. 4.) With regards to Guideline 9.13, one respondent suggested that the frequency and the intensity of transaction monitoring should increase with enhanced due diligence. One respondent also suggested to clarify on which legal basis firms should identify and verify the identity of other shareholders. 5.) With regards to Guideline 9.16, one respondent asked to delete the guideline completely. Another respondent was	The suggestion is not related to any of the revisions to the guidelines that was proposed in the CP and therefore out of scope of the consultation.	*None*

	considering the CDD measures as not applicable to clients who opened and held an account.		
Feedback on responses to Question 10 (electronic money issuers)			
Guideline 10	While acknowledging guidelines 4.9 to 4.11 recognising the need to balance financial inclusion against mitigating ML/TF risks, one respondent asked the EBA to explicitly acknowledge the consideration of financial inclusion in the sectoral guidelines 10.	Financial inclusion with regards to prepaid cards is explicitly included in recital 14 of AMLD. At the same time, financial inclusion is adequately considered throughout the guidelines.	*None*
Guideline 10	One respondent commented that some electronic money products are created to support sections of the population which are unbanked or who have less access to traditional banking products. Due diligence and monitoring for such customers need to take into account financial inclusion and a risk-based approach for EMI firms.	The EBA sets clear expectations regarding financial inclusion in these guidelines that apply to electronic money products as they do to other financial products and services. Firms should remain mindful that financial exclusion is not, of itself, indicative of lower ML/TF risk and that appropriate risk-mitigation remains essential in all cases.	*None*
Guideline 10.8 a)	According to several respondents, the reference to electronic identification 'documents' seemed inaccurate as Article 3(2) of Regulation (EU) No 910/2014 defines electronic identification 'means', not 'documents'.	Having assessed the consultation responses, the EBA agrees that the guidelines should be in line with Article 3(2) of Regulation (EU) No 910/2014 with regards to 'electronic identification means'. The EBA has therefore amended the guideline and for the sake of consistency, implemented similar changes in guidelines 9.10 a); 14.10 a) and 17.7 a).	*'10.8 a): Online and non-face-to-face distribution without adequate safeguards, such as electronic signatures, electronic identification means ~~documents~~ meeting the criteria set out in Regulation (EU) No 910/2014 and anti-impersonation fraud measures.'*
Guideline 10.9	One responded mentioned that the additions to Guideline 10.9 represented a material change to the current guidelines. The respondent considered such a fundamental change not fully justified. The respondent would strongly advocate for a risk-based approach to be applied to instances where an agreement is entered into based on the risk profile of the merchant. One respondent suggested, with regards to the second sentence, considering also the use of crowdfunding platforms.	The risk-based approach is reflected throughout the guidelines and applies also to Guideline 10.9. The Guideline focusses on distribution agreements between electronic money issuers and merchants and requires that firms should understand the nature and purpose of the merchant's business to satisfy themselves that the goods and services provided are legitimate and to assess the ML/TF risk associated with the merchant's business. The Guideline also contains specific	*None*

		clarifications for online merchants. In this context, an addition of the example of crowdfunding platforms is not necessary.	
Guideline 10.9	One respondent assumed that the reference to a 'distribution agreement' is a reference to a merchant acquiring agreement for e-money services, rather than an agreement for the distribution of e-money. One respondent commented that customers might not declare, before opening a new account, the expected volume of transactions to be carried through the payment account or a POS for electronic payments. It was more effective analysing the volume carried out in the payment account after a certain period of time (e.g. 1 year after the activation of the payment account) in order to evaluate the consistency of relevant deviation of customer's behaviours from his usual patterns. In addition, it was suggested focusing on the KYC process to understand from the client the intended use of the payment account, irrespective of the expected volume of transactions.	The Guideline requires that firms need to understand the nature and the purpose of the merchant's business. Guideline 4 is clear that establishing the expected volume and nature of transactions upfront helps firms establish the nature and purpose of the business relationship, and subsequently to monitor transactions in a meaningful and sufficiently effective way. The Guidelines are clear that risk assessment and management is an ongoing process, and the knowledge a firm has of its customer will evolve as the relationship progresses and matures.	*None*
Guideline 10.11 a)	According to one respondent, the owner of the e-money has been identified as the focus of CDD measures, subject to an existing business relationship with the customer, or the customer undertaking qualifying occasional transaction(s). Reference to triggers for verification would be helpful.	Guideline 10.11 states that firms should apply CDD measures to the owner of the electronic money account or product and to additional card holders. Further clarifications are not necessary for the purpose of this Guideline. Firms should apply Guideline 10 in conjunction with Title I of the Risk Factors Guidelines.	*None*
Guideline 10.11 b)	According to one respondent, it would be helpful to clarify when the existence of additional card holders could be an indicator of having entered into more than one business relationship or that these additional card holders could be beneficial owners. In addition, it was not clear why it was required to identify whether the card holder could be beneficial owner.	Firms should assess whether additional card holders are customers or beneficial owners, based on their business model and provisions in the AMLD.	*None*
Guideline 10.15	One respondent mentioned that it could be elaborated to state that EDD is a risk-based requirement and that the assessment must be subject to a full range of factors including the product proposition. One respondent noted that it is common practice for financial institutions to apply enhanced due diligence measures to high-risk	As stated in Guideline 10.15, firms should refer to Title I of the Risk Factors Guidelines. Article 18a of the AMLD requires specific EDD measures in the context of high-risk third countries.	*None*

	third country transactions or customers, in line with a risk-based approach. The respondent believed that not every transaction or firm from a high-risk third country should be automatically subject to full enhanced due diligence, but obliged entities should ensure that high-risk third country transactions are adequately addressed. The respondent therefore requested that the guidelines should be flexible enough to allow additional aspects to be considered. More generally, the respondent requested that the high-risk third country lists to be aligned globally to ensure consistency, and welcomed the European Commission's recent efforts in this respect.		
Guideline 10.18 a)	Several respondents commented that guideline 10.18 a) addressed the postponement of the verification of a customer's identity. They believed the inclusion of the EUR 150 monetary threshold went against the drive for a pragmatic, risk-based approach to SDD. No monetary threshold should be set, noting that it did not allow for any mitigating measures to be taken into account. Recital 7 of AMLD made it clear to the respondent that in the event the Article 12 of AMLD exemption did not apply, e-money issuers should be able to benefit from the SDD provisions in Article 15, subject to the risk being low. Article 15 did not include any monetary limit and the respondents believed the proposed threshold in the guideline is unnecessarily restrictive, disproportionate and contrary to the benefits of a risk-based approach. Respondents strongly urge the EBA to consider the removal of the monetary limit.	The threshold of EUR 150 reflects the threshold in Article 12 of AMLD. The EBA notes that the guidance in Guideline 10.18 a) is one of a number of SDD measures that issuers may apply in lower risk situations and issuers are able to choose the SDD measure that best reflects their situation, and that of their customers.	*None*
Summary of responses out of scope	1.) With regards to guidelines 10.4, 10.5 and 10.6, several respondents queried a number of risk factors. 2.) With regards to guideline 10.8 a), several respondents suggested that it should be specified that the certificate shall be an advanced electronic signature. 3.) With regards to guideline 10.14, one respondent requested further clarification on the examples of the types of monitoring systems.	The suggestion is not related to any of the revisions to the guidelines that was proposed in the CP and therefore out of scope of the consultation.	*None*

	4.) With regards to guideline 10.18 f), one respondent remarked that, if a gift card or other prepaid product exclusively is accepted as a payment instrument by the issuer himself (closed-loop), the product cannot be classified as e-money.		
Feedback on responses to Question 11 (money remitters)			
Guideline 11.11 a)	According to one respondent, the country of an IP address was not by itself a factor that led to a higher ML/TF risk. As a consequence, the respondent suggested deleting from the guideline 11.11 the part mentioning *'or the transaction is executed from an IP address'*.	The Guideline is clear that an IP address is not, of itself, an indicator of higher risk but it can be a useful indicator of links to jurisdictions where further consideration might be necessary.	*None*
Summary of responses out of scope	1.) With regards to guideline 11.5, two respondents suggested to add virtual currencies, given that a transaction funded with virtual currency could contribute to increase the ML/TF risks. 2.) With regards to guideline 11.13 c), one respondent suggested the deletion of the guideline.	The suggestion is not related to any of the revisions to the guidelines that was proposed in the CP and therefore out of scope of the consultation.	*None*
Feedback on responses to Question 12 (wealth management)			
Guideline 12.8 b)	One respondent proposed that the source of funds could also be verified using a recent tax return statement.	The EBA welcomes the respondent's suggestion. The listing presented in Guideline 12.8 b) for verifying the source of funds or wealth is not exhaustive. It should be understood as an enumeration of possibilities that are meant to provide support / guidance for the user. In case a certified tax statement represents the true and valid source of funds, the usage as a verification document can be considered.	*None*
Guideline 12.8 b)	One respondent suggested a list of sources of information that can be used to establish the source of funds and source of wealth. This information would then be used to confirm PEPs, too.	The EBA's list of possible sources is not exhaustive and firms can use other information sources as appropriate. The sources of information set out in this Guideline are particularly relevant in the context of wealth management under guideline 12 and complement those in the general part of the Guidelines.	*None*

	Moreover, the respondent recommends that the guideline should be included under the Enhanced Due Diligence Guidelines in guideline 4.		
Guideline 12.8 b) viii) and ix)	One respondent suggested that the guidelines should be subject to two different subsections of guideline 12.8 in line with AMLD. This respondent mentioned as a background that the obligation to 'establish the destination of funds' was not required by AMLD. Thus exact wording of the Directive: 'obtaining information on the reasons for the intended or performed transactions;' should be used instead of adding a new requirement.	Guideline 12.8 refers to the EDD measures set out in Article 18a of the AMLD and to Title I of the Guidelines (guidelines 4.53 to 4.57). The EBA agrees that establishing the destination of funds does not form part of firms' efforts to verify the source of wealth or source of funds. The destination of funds needs to be assessed by the firm separately, as it is an important risk assessment tool. The fact that the destination of fund is a high-risk third country, thereby implicitly requires firms to verify the destination of funds. In order to make this point more pronounced, both for high risk third countries and more in general, the EBA has amended Guideline 12.7 and 12.8 to reflect this assessment of the destination of funds.	*Guideline 12.7 :* *'[...] The relationship manager's close contact with the customer will facilitate the collection of information that allows a fuller picture of the purpose and nature of the customer's business to be formed (e.g. an understanding of the client's source of wealth, the destination of funds, why complex or unusual arrangements may nonetheless be genuine and legitimate, or why extra security may be appropriate).'* *Guideline 12.8:* *'To comply with Article 18a in respect of relationships or transactions involving high-risk third countries, firms should apply the EDD measures set out in this regard in Title I. (…)* *b) ~~viii) Establishing the destination of funds.~~* *c): Establishing the destination of funds.*

Summary of responses out of scope	1.) With regards to guidelines 12.4 and 12.6, several respondents queried a number of risk factors. 2.) With regards to guideline 12.8 a), one respondent asked for clarification to which extend 'more information about clients' is satisfied and which expectations towards banks do exist.	The suggestion is not related to any of the revisions to the guidelines that was proposed in the CP and therefore out of scope of the consultation.	*None*
Feedback on responses to Question 13 (trade finance providers)			
Guideline 13.10 d) and g)	Many respondents commented on the revisions to guideline 13.10 d) and g) where factors have been added that point to increased risk. The revised guideline mentions that factors that may contribute to increasing risk are d) if there are significant discrepancies in documentation or g) if the agreed value is over- or underinsured or multiple insurances are used. Respondents argued that credit institutions generally do not inspect the actual goods. Furthermore, respondents argued they are not in a position to determine over or underinsurance in line with the revised guideline 13.10 g) so could only assess this to the extent it is known.	With respect to the revised guideline 13.10d), EBA notes that the 'Transaction Risk Factors' did not change. The revision only provides a new example, by adding that if a trade finance provider identifies significant discrepancies, *for instance* between the description of (the type, quality or quantity of the) goods and actual goods shipped, this could be relevant to the extent this is known. The guideline do not request firms to actually inspect all goods per se. With regard to Guideline 13.10g) the revised guideline now includes an additional risk factor, namely when the agreed value of goods or shipment is over- or underinsured or multiple insurances are used. Further to respondent's comment, the EBA believes a similar caveat is justified as under the revised guideline 13.10 d) to increase consistency and better reflect common practices, by adding, 'to the extent this is known'. For more trends and developments in Trade Based Money Laundering, please refer to the recent report by FATF together with Egmont Group of Financial Intelligence Units, published December 2020.	*'13.10. g): The agreed value of goods or shipment is over- or under-insured or multiple insurances are used, to the extent this is known.'*
Guideline 13.10 h)	One respondent raised that dual-use items mentioned in 13.10 h) may be very numerous and cannot be considered in themselves as an 'AML red flag'. Respondent argues they should be analysed in the context of a sensitive final use or final user, where the goods transacted require export licenses, such as specific export authorizations for dual-use items.	The revised Guideline 13.10 h) provides that goods that require export licenses, such as specific export licenses for dual-use items' may be indicative of higher ML/TF risk. In line with the Guidelines principles, firms should take a holistic view of all risk factors as one single risk factor does not necessarily push the entire relationship into a higher or lower risk category. For dual-use items that need a specific export authorization, firms need to consider the risk related to it as transaction risk factor.). The	*None*

		footnote provides further details what is meant with dual-use items.	
Guideline 13.10 l)	One respondent asks for further clarification on the new guideline 13.10 l) that states '*The goods traded are destined to an embargoed country, to a prohibited end user, or in support of a prohibited end-user*.' Respondent states further guidance is required on the definition of 'prohibited end-user'.	The EBA has made editorial changes to clarify this relates to goods destined to parties or countries that are under sanctions, embargos or similar measures issued by, for example, the Union or the United Nations, similar to Annex III 3(c) AMLD.	*13.10 l) The goods traded are destined to a party or country that is subject to a sanction, an embargo or a similar measure issued by, for example, the Union or the United Nations, or in support of such party or country. ~~an embargoed country, to a prohibited end user, or in support of a prohibited end user~~*
Guideline 13.11 a)	Respondent argues that it is difficult for credit institutions to assess the suitability and reliability of independent inspection agents, both where it comes to verification of goods and the necessary documents and authorizations. The respondent asks for more guidance on who qualifies as independent agent, and whether such agent should be authorized or certified.	The comment relates to Guideline 13.11 a) where an addition has been made to the factors that may contribute to reducing risk. Under the revised guideline, in order to consider risk reduction, the independent agent should not only verify the quality and quantity of the goods but also the 'presence of the necessary documents and authorizations'. EBA does not propose any changes to the concept of independent agent itself, or impose any new criteria which agents qualify as independent agent (e.g. by requesting a certification or authorization).	*None*
Summary of responses out of scope	1.) With regards to guideline 13.14 b), one respondent suggests to add countries that are listed as 'non-cooperative jurisdiction for tax purposes'. 2.) With regards to guideline 13.15 a), one respondent suggests to remove the particular risk factor that trade is within the EU/EEA especially considering tax carousel fraud. 3.) With regards to guidelines 13.20 to 13.22, two respondents indicate these additional checks are challenging in practice, would increase complexity and in some cases be impossible. One respondent requests to add 'if possible' to the guidelines and to delete particular expectations.	The suggestion is not related to any of the revisions to the guidelines that was proposed in the CP and therefore out of scope of the consultation.	*None*

Feedback on responses to Question 14 (life insurance undertakings)			
General comment relating to Guideline 14	One respondent stressed to keep in mind key points when finalizing the update (cash payments were still not necessarily unusual in some markets, and anonymity was not usually possible in European insurance contracts).	The Guidelines set out that cash payments are considered a higher risk compared to other means of payment, and set out that in case there is anonymity, it should be considered as a higher risk factor.	*None*
Guideline 14.7 l)	One respondent raised that there could be other conditions to be met to benefit from tax relief, that can also refrain the use of the product for money laundering purposes. It is therefore unnecessary to restrict the scope of this risk-reducing factor.	Benefiting from tax relief is not a risk reducing factor. The risk factor that may contribute to reducing risk focusses, in the context of tax reliefs, on products having conditions limiting the availability of funds.	*None*
Guideline 14.9	One respondent questioned which simplified measures the insurance undertaking should adopt on credit or financial institutions, in particular when the Bank was the policyholder of different collective policies and if it could be possible to avoid the customer due diligence on these subjects, which are supervised by independent Authorities and which are, in their turn, obliged subject under AML European and local rules.	Guideline 14.9 does not specify which measures undertakings should apply in the case a bank is the policyholder. It only highlights situations where the risk associated with the business relationship may be reduced.	*None*
Guideline 14.10 a)	Two respondents suggested replacing the reference to 'electronic signature' by 'qualified certificate for electronic signatures'. Furthermore, they raised that the reference to electronic identification 'documents' seems inaccurate; Regulation (EU) No 910/2014 concerned electronic identification 'means'. One respondent stressed that the consistency of the CDD with the proceeding provided explicitly by the local Regulators for non-face-to-face identification should be considered as factors which may contribute to reducing risk.	The EBA notes that in the context of an electronic identification the Guidelines do not require a 'qualified certificate for electronic signature', in light with the principle of proportionality. However, the EBA is of the view that the Guidelines should be in line with Article 3(2) of Regulation (EU) No 910/2014 (eIDAS Regulation) with regards to 'electronic identification means'. The EBA has therefore amended the guideline and for the sake of consistency, implemented similar changes in Guidelines 9.10 a); 10.8 a) and 17.7 a). Furthermore, guideline 4.29 b) clarifies that 'Firms should assess whether the non-face to face nature of the relationship or occasional transaction gives rise to increased ML/TF risk and if so, adjust their CDD measures accordingly.'	*'14.10 a) non-face-to-face sales, such as online, postal or telephone sales, without adequate safeguards, such as electronic signatures or electronic identification ~~documents~~ means that comply with Regulation (EU) No 910/2014;'*
Guideline 14.11	One respondent stressed that the guideline could be useful for intermediaries in combination with the general guidance provided under Title 1 of the EBA Guidelines and with guideline 14.11 that	The EBA took note of the comment. The respondent did not suggest any changes to the guidelines.	*None*

	ML risk may be reduced when intermediaries are well known to the insurer, who is satisfied that they duly comply with the CDD requirements.		
Guideline 14.16	One respondent noted that guidance 14.16 amended the current guidance 190, by including a reference to the beneficiary and was therefore of the view that this seemed to go beyond the requirements of AMLD.	The EBA agrees with the concern raised. For clarification, the guideline has been aligned to AMLD.	*'14.16: Where the firm knows that the life insurance has been assigned to a third party, who will receive the value of the policy, they must identify the ~~beneficiary and~~ the beneficial owner ~~of the beneficiary~~ at the time of the assignment.'*
Guideline 14.21	One respondent noted that it should be allowed for insurance undertakings to adopt simplified or ordinary CDD measures on the beneficiary until the time of pay-out. The respondent also noted that the same guideline has been included in Guideline 14.22.	Guideline 14.21 only applies if the beneficiary is already known at a certain stage in the insurance contract and has been identified as a PEP. Under these circumstances, Article 20 of AMLD4 specifies that enhanced scrutiny of the entire business relationship with the policyholder should be conducted. This is independent from the time of pay-out. However, the EBA agrees that Guideline 14.22 is a duplication of 14.21, and that it therefore deletes guideline 14.22.	*~~14.22. Where the beneficiary is a PEP and is expressly named, firms should not wait until the payout of the policy to conduct the enhanced scrutiny of the entire business relationship.~~*
Summary of responses out of scope	1.) With regards to guideline 14.6 b), one respondent queried the particular risk factor. 2.) One respondent suggested amending guideline 14.14 so that the application of the CDD measures was only relative to the client contracting the insurance. 3.) With regards to guideline 14.16, one respondent suggested adding an additional clarification.	The suggestion is not related to any of the revisions to the guidelines that was proposed in the CP and therefore out of scope of the consultation.	*None*
Feedback on responses to Question 15 (investment firms)			
Guideline 15 (General comment)	Several respondents considered that the guideline should take into account that some jurisdictions are providing strong AML/CFT	While the EBA notes that there is no general third country equivalence regime with regards to the AML/CFT requirements in AML5, EBA also highlights that the nature of the AML/CFT regimes of the individual jurisdictions can be taken into account in	*None*

	regimes, or equivalent to the European requirements in combating ML/TF, which may also contribute to lower the risk.	individual assessment of the ML/TF risk. As this is not a specific issue related to the individual sector, the issue is addressed in general section of the Guidelines (guideline 2.12) that clarifies, that to the extent permitted by national legislation, firms should be able to identify lower risk jurisdictions in line with these guidelines and Annex II of AMLD.	
Guideline 15 (General comment)	One respondent suggested to add an explicit reference to the requirements of AMLD in guideline 15.	The EBA notes that the link is established in the general section of the guidelines, and as such does not need to be repeated in each sectoral guideline.	*None*
Guideline 15 (General comment)	One responded commented that it is necessary to adapt the AML/CFT regulatory framework to the specificities of the investment services sector.	EBA notes that within the remit of the requirements of the AMLD the sectoral guideline 15 takes into account the specificities of the investment services sector. Specific guidance on identification of customers (including guidance on intermediaries) is included in guideline 16.	*None*
Guideline 15.1 and Definitions	One respondent suggested to add a definition of an investment firm.	As investment firm is defined directly in MiFID II, EBA considers that adding a link in guideline 15.1 to specific article of MiFID II can improve readability of the Guidelines.	*'15.1: […] as defined in point (1) of Article 4(1) of Directive 2014/65/EU […]'*
Guideline 15.3 c)	One respondent suggested to remove reference to 'that appear unusual' in guideline 15.3(c) for mirror trades as it might be unclear to what this is captured	The EBA considers that the reference to transactions that appear unusual is useful to capture transactions which characteristics (e.g. frequency, size, structure or pattern of conduct) might indicate higher risk related to the products, services or transactions. This might include also transactions that facilitate currency exchange, particularly for non-standard or high-risk currencies or transactions that are outside of the expected business activity of such customer (e.g. considering the customer's profile). EBA notes that the concept of unusual is used in AMLD and further explored throughout the Guidelines, including in Guideline 4.	*None*
Guideline 15.3 d)	Two respondents commented that structured products should not be considered as a factor of increasing risk.	EBA agrees that not all structured products automatically imply increased AML risk. However, the Guidelines specifically refer to products or services that are structured in a way that may present difficulties in identifying the customers. In EBA's view, such	*None*

		structuring may be indicative of increased money laundering risks.	
Guideline 15.5c	Several respondents to the consultation disagreed that all the specific examples of the sectors of customers business in guideline 15.5 c) are to be considered high risk.	The EBA considers that the examples of industries with higher risk included in the guidelines remain valid and consistent with those set out in the general part of the Guidelines. The Guidelines are clear that firms should take a holistic view of all risk factors as a single risk factor may not push a relationship into a higher or lower risk category. The firm needs to consider the factors and be able to demonstrate to its competent authority that the measures taken are adequate in view of the ML/TF risk.	*None*
Guideline 15.6	Three respondents suggested to add listed companies as a specific factor which may contribute to reducing customer risk in guideline 15.6.	EBA notes that Annex II to AMLD considers public companies listed on a stock exchange and subject to disclosure requirements, which impose requirements to ensure adequate transparency of beneficial ownership as one of the factors of potentially lower risk. As this factor is specifically stated in said Directive and addressed in the general part of the guidelines (Guideline 2.4(g)), the EBA considers it is not necessary to repeat this consideration in each individual sectoral guideline. Instead and in order to achieve consistency among the sectoral guidelines, specific reference to listed companies have been removed from guidelines 13, 14 and 20. No change is needed for Guideline 15.6.	*None to guideline 15.6. However, consequential amendments to the following guidelines:* *'13.13 b): The following factors may contribute to reducing risk: [..];* ~~*The customer is listed on a stock exchange with disclosure requirements similar to the EU's.*~~ *'14.9 b): The following factors may contribute to reducing risk. In the case of corporate-owned life insurance, the customer is:* ~~*b. a public company listed on a stock exchange and subject to regulatory disclosure requirements (either by stock exchange rules or through law or enforceable means) that impose requirements to ensure adequate transparency of beneficial*~~

			~~*ownership, or a majority-owned subsidiary of such a company.'*~~ *'20.4: The customer is:* ~~*a) 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.'*~~
Guideline 15.7 c)	Two respondents highlighted that investment firms might not always have information about the location of the participants of the trading venue.	The EBA considers that firms should consider this risk factor to the extent it is known and that firms may obtain this information as part of their general customer due diligence and know your customer efforts.	*None*
Guideline 15.9	One respondent suggested clarification that reference to MiFID in guideline 15.9 refers to MiFID II.	EBA has amended the Guideline accordingly.	*'15.9: […] the extent to which information obtained for MiFID II and EMIR compliance […]'.*
Guideline 15.9	With regards to reference to information collected for MiFID II and EMIR compliance purposes in guideline 15.9, two respondents questioned whether such reference should be retained as all available information is used, while other respondent specifically agreed that such information can be used for meeting customer due diligence requirements.	The purpose of this Guideline is to highlight that information firms will obtain to comply with their obligations under MIFID and EMIR can also be helpful in meeting their AML/CFT obligations.	*None*
Summary of responses out of scope	With regards to guidelines 15.5 and 15.6, several respondents suggested changes to the wording of factors increasing and reducing risk.	The suggestion is not related to any of the revisions to the guidelines that was proposed in the CP and therefore out of scope of the consultation.	*None*

Feedback on responses to Question 16 (providers of investment funds)			
Guideline 16	One respondent suggested that reference made to equivalent third countries should be harmonized throughout these guidelines.	While the EBA notes that there is no general third country equivalence regime with regards to the AML/CFT requirements in AMLD, EBA also highlights that the nature of the AML/CFT regimes of the individual jurisdictions can be taken into account in individual assessment of the ML/TF risk. As this is not a specific issue related to the individual sector, the issue is addressed in general section of the Guidelines (guideline 2.12) that clarifies, that to the extent permitted by national legislation, firms should be able to identify lower risk jurisdictions in line with these guidelines and Annex II of AMLD.	*None*
Guideline 16.3 b)	Respondents also suggested that the Guidelines should be more specific when mentioning AIFs that had an inherently higher risks by restricting point b) to those AIFs with small number of investors.	The Guidelines are clear that point b) only targets funds with smaller number of investors, as some hedge funds, some (not all) real estate and some (not all) private equity funds may be. However, the EBA notes that in Guideline 16.3 b) accidently one word was missing and therefore adds the word 'such'.	*'16.3 b) Alternative investment funds, such as hedge funds, real estate and private equity funds, tend to have a smaller number of investors, which can be private individuals as well as institutional investors (pension funds, funds of funds). Such funds that are designed for a limited number of high-net-worth individuals, or for family offices, […].'*
Guideline 16.5 b)	According to two respondents, the possibility to redeem fund shares without incurring in significant administrative costs is both a central right of investors in a fund and normal practice for short-term investments. Therefore it cannot be listed as an increased risk factor.	EBA notes that these parts of the Guidelines were not subject to consultation. EBA considers, though, that funds allowing quick and easy subscription/redemption are, in general, riskier than those with lock-up period. EBA also agrees that some funds can be very short-term and in such case, early and quick redemptions may be considered as normal. However it is EBA's view not to provide case by case analysis in the guidelines.	*None*
Guideline 16.9 and 16.11	Three respondents suggested to add listed companies as a specific factor which may contribute to reducing customer risk as well as	EBA notes that Annex II to AMLD considers public companies listed on a stock exchange and subject to disclosure requirements, which impose requirements to ensure adequate	*None*

	distribution channel risks in Guidelines 16.9 and 16.11 respectively.	transparency of beneficial ownership as one of the factors of potentially lower risk. As this factor is specifically stated in the Directive and addressed in the general part of the Guidelines (guideline 2.4 j), EBA considers it is not necessary to repeat this consideration in each individual sectoral guideline.	
Guideline 16.13	Three respondents considered it worth replacing 'investor' in line 6 by 'customer' as the customer is the only one that can be asked as to whether it invests on its own account of or if it is an intermediary that invests on behalf of a final investor.	EBA agrees with this comment and introduces a minor clarification to the text which does not change the meaning of the Guideline.	*'16.13 […] The fund or fund manager should also take risk-sensitive measures to identify and verify the identity of the natural persons, if any, who ultimately own or control the customer (or on whose behalf the transaction is being conducted), for example by asking the prospective ~~investor~~ customer to declare, when they first apply to join the fund, whether they are investing on their own behalf or whether they are an intermediary investing on someone else's behalf.'*
Guideline 16.14	One respondent suggests to align the definitions of points a) and b) with reference to the funds' register (as mentioned in point c).	The various definitions take into account not only the register criteria but also how the customer/investor comes to the fund, in order to be as exhaustive as possible. EBA considered that the suggested amendment would leave some situations uncovered.	*None*
Guidelines 16.17 and 16.20	Three respondents flagged a mismatch between guideline 16.17 and guideline 16.20, leading to a misunderstanding as to the situations where enhanced due diligence are required and simplified due diligence allowed. In particular, the reference made to 'relationship similar to correspondent banking' that is unusual in the funds management industry.	Guideline 16.17 was reviewed to align it with the FATF Risk-Based Approach for the securities sector and in particular to provisions relating to cross-border relationship similar to correspondent banking established for securities transactions or funds transfers. The Interpretative Note on the FATF Recommendation on correspondent banking does not give further guidance on what constitutes a "relationship similar to correspondent banking" since it only states that "The similar relationships to which	*None*

		financial institutions should apply criteria (a) to (e) include, for example those established for securities transactions or funds transfers, whether for the cross-border financial institution as principal or for its customers." The guideline 16.17 recalls the possibility that firms consider their business relationship as "similar to correspondent banking" (possibly relying on further indications contained in their respective national legislation) and therefore decide to apply EDD measures to their respondent. If, on the contrary, firms do not consider this condition to be met, they may also decide to apply measures provided in guideline 16.20.	
Guideline 16.20	Several respondents considered unclear to whom the customer due diligence measures apply under Guideline 16.20.	In EBA's view, Guideline 16.20 addresses the situation where customer due diligence measures must be both applied towards the financial intermediary as a customer and the final investors as beneficial owner of the funds while allowing funds managers to apply simplified due diligence measures towards the final intermediary only subject to the a) to e) conditions. Outside this low-risk situation, the fund manager should take risk sensitive measures to identify, and where relevant, verify the identity of, the investors underlying customers of the financial intermediary that invest in the fund, as these investors customers may increase the implied risk associated with could be beneficial owners of the funds invested through the intermediary.	*None*
Summary of responses out of scope	1.) With regards to guidelines 16.3, 16.5, 16.10 and 16.11, several respondents queried a number of risk factors. 2.) With regards to guidelines 16.20 e), three respondents suggested lightening the guideline regarding access to the customers' files of the financial intermediary.	The suggestion is not related to any of the revisions to the guidelines that was proposed in the CP and therefore out of scope of the consultation.	*None*
Feedback on responses to Question 17 (crowdfunding)			
Guideline 17	Many respondents stated that they did not have any comments on the additional sector-specific Guideline 17 on crowdfunding platforms.	After finalising the Consultation Paper, Regulation (EU) 2020/1503 on European crowdfunding service providers for business has been published. As mentioned in the Consultation Paper, the EBA has amended guideline 17.1 in order to reflect the relevant definitions provided in that Regulation. The EBA has also	*Guideline 17.1:* *17.1. <u>For the purposes of this sectoral Guideline, the following definitions set out in Article 2(1) of Regulation (EU)</u>*

		clarified that guideline 17 refers to 'customers' in the meaning of 'clients' as defined in Regulation (EU) 2020/1503. Furthermore, the EBA has removed the redundant guideline 17.13.	*2020/1503 are used and should apply: 'crowdfunding service', 'crowdfunding platform', 'crowdfunding service provider' (CSP), 'project owner' and 'investor'. This sectoral Guideline refers to 'customers' in the meaning of 'clients', as defined in Article 2(1) (g) of that same regulation.* *Guideline 17.13 has been removed.*
Guideline 17.5 a)	One respondent asked for clarification and further justification as the guideline seemed to create a form of reliance on banks that did not exist in interbank relations.	Guideline 17 should be read together with Title I of the Risk Factors Guidelines that contains additional requirements for CSPs. Guideline 17.5 a) therefore, as one risk factor among others to be considered, does not imply an inappropriate reliance on credit institutions.	*None*
Guideline 17.5 f)	One respondent asked for clarification as the guideline limited the business model of CSPs, even though it was true that ML schemes could be facilitated by the creation of several accounts by the same person under straw men names or shell companies.	Guideline 17.5 f) highlights a potentially risk-reducing factor, and does not limit the business model of CSPs.	*None*
Guideline 17.7 a)	Two respondents asked for stricter safeguards ('advanced electronic signature' and 'qualified certificate for electronic signature') and mentioned that the reference to 'electronic identification documents' seemed to be inaccurate as Regulation (EU) No 910/2014 defined 'electronic identification means'.	The EBA notes that in the context of an electronic identification the Guidelines do not require an 'advanced electronic signature' or a 'qualified certificate for electronic signature', in light with the principle of proportionality. However, the EBA is of the view that the Guidelines should be in line with Article 3(2) of Regulation (EU) No 910/2014 (eIDAS Regulation) with regards to 'electronic identification means'. The EBA has therefore amended the guideline and for the sake of consistency, implemented similar changes in Guidelines 9.10 a); 10.8 a) and 14.10 a).	*'17.7 [..] a) The CSP operates the crowdfunding platform entirely online without adequate safeguards, such as electronic identification of a person using electronic signatures or electronic identification ~~documents~~ means that comply with Regulation (EU) No 910/2014.'*

Guideline 17.16	One respondent suggested another wording as a clarification ('CSPs must not rely on credit institutions or financial institutions to satisfy themselves that these credit institutions or financial institutions have put in place appropriate CDD measures if there is not an agreement between them to delegate the application of CDD measures').	Guideline 17.15 states that CSPs that are subject to AML/CFT requirements should apply CDD measures in line with Title I of the Risk Factors Guidelines to all their customers, be those investors or project owners. Guideline 17.16 states that CSPs that rely on credit institutions or financial institutions to collect funds from or transfer funds to customer should refer to the distribution channel risk factors in Title I of the Risk Factors Guidelines and in particular, satisfy themselves that these credit institutions or financial institutions have put in place appropriate CDD measures. CSPs remain ultimately responsible for any failure to comply with their CDD obligations.	*None*
Feedback on responses to Question 18 (account information and payment initiation service providers)			
Guideline 18 Guideline 18.2	Several respondents mentioned that AISPs and PISPs should not be considered as obliged entities under AMLD. Respondents stated different reasons for this request, such as a low or non-existent ML/TF risk and a disproportionate duplication of the AML checks carried out by ASPSPs. Respondents also queried whether the inclusion of AISPs and PISPs as obliged entities under the AMLD was intentional, or whether this was an unintentional result of cross referencing between the AMLD Directive (EU) 2015/2366 (PSD2) and Directive 2013/36/EU (CRD). Several respondents asked the EBA not to finalise the additional sector-specific guidelines 18 until the European Commission published proposals for a future EU AML/CFT framework. Furthermore, several respondents raised concerns that the requirements in the guidelines for AISPs and PISPs would put AISPs and PISPs in breach of their obligations under Articles 66 and 67 of PSD2, as the data would be used for a different purpose than as allowed under this Directive.	EU law defines AISPs and PISPs as obliged entities, more specifically under Article 2 AMLD. The EBA is not in the position to change EU law. Equally, the EBA recently provided advice to the European Commission (EC) on a future EU AML/CFT framework (EBA/OP/2020/14 and EBA/REP/2020/25), recommending to the EC to further assess the inclusion of AISPs as obliged entities. The EBA acknowledged that the inherent ML/TF risk associated with AISPs and PISPs is limited. The final guidelines acknowledge that AISPs and PISPs are obliged entities under AMLD and seeks to reach a proportionate approach as regards the AML/CFT obligations that arise as a result of this provision, taking into account the limited ML/FT risk associated with the provision of their services. With regard to the suggestion for the EBA to consider delaying guideline 18 until the EC has published its proposals for a future EU AML/CFT framework, the EBA notes that it might take several years until the new framework will have been negotiated, published and eventually will legally apply. The EBA does not await events in such distant future but fulfils its objectives and tasks under the legal framework applicable at any given point time. This includes the revision of Guidelines that take into	*None*

		account other EU Directives that came into being since the original Guidelines were published. With regards to the permitted use of data by AISPs and PISPs under PSD2, and, in general, data protection related aspects, the EBA refers, in particular, to recital 43 and the requirements in Articles 40, 41 and 43 of AMLD. These requirements are complementary, and without prejudice, to the obligations applicable to AISPs and PISPs under the PSD2. There is therefore no conflict between the guidelines and the PSD2.	
Guideline 18	Several respondents requested that the EBA should publish additional Draft Regulatory Technical Standards on the access to data for AISPs and PISPs in the context of the AMLD and the PSD2.	With regards to AISPs' and PISPs' rights and obligations concerning access to customers' payment accounts data set out in PSD2, these are also explained in Commission Delegated Regulation (EU) 2018/389 (the EBA RTS on SCA & CSC). Furthermore, additional clarifications have been published by the EBA especially in its opinions EBA-Op-2018-04 (Opinion on the implementation of the RTS on SCA and CSC) and EBA/OP/2020/10 (Opinion on obstacles under Article 32(3) of the RTS on SCA and CSC), and via the EBA's 'Q&A tool'.	*None*
Guideline 18.3 Guideline 18.10	Several respondents queried the structure of Guidelines 18, including references to Title I of the Guidelines, and requested clarifications which SDD measures should be applied.	As stated in Title I of the guidelines, these guidelines come in two parts. Title I is general and applies to all firms. Title II is sector-specific, incomplete on its own and should be read in conjunction with Title I. Guideline 18.3 reiterates this structure, specifying that, when offering payment initiation services or account information services, PISPs and AISPs should take into account, together with Title I, the provision set out in guideline 18. CDD, EDD and SDD measures are further described in guidelines 18.8 to 18.15. For completeness, in the case Payment Service Providers (also) offer other payment services, they should apply other relevant sector-specific Risk Factors Guidelines when providing those other payment services.	*None*
Guideline 18.5	One respondent stated that the ESAs' Opinion on the use of innovative solutions by credit and financial institutions in the customer due diligence process (JC 2017 81) did not provide context on distribution channel risk factors. This respondent	The respondent refers to the ESAs' opinion that has been published in 2018 and that is addressed to competent authorities. Having assessed the consultation response, the EBA agrees that	*Guideline 18.5:* *When assessing ML/TF risks, PISPs and AISPs ~~should take~~*

	proposed to include a reference on how transactional data could be imported and analysed at the point of on-boarding for the purpose of CDD.	additional clarification would be useful. It has therefore amended the guideline accordingly.	~~*into account*~~ *may wish to refer to the ESAs' Opinion on the use of innovative solution in the customer due diligence process the use of innovative solution in the customer due diligence process.'*
Guideline 18.1 Guideline 18.5 Guideline 18.8 Guideline 18.10 Guideline 18.12	Many respondents were of the view that the draft guidelines did not reasonably reflect the (different) business models of AISPs and PISPs. With regards to Guideline 18.1, one respondent mentioned that it appeared that the guideline was applicable without distinction to PISPs and AISPs, and did not take into account the different ML/TF risk level associated with the provision of AIS compared to PIS. With regards to Guideline 18.5, one respondent stated that the ESAs' Opinion on the use of innovative solutions by credit and financial institutions in the customer due diligence process (JC 2017 81) acknowledged that CDD was often associated with significant cost and customer inconvenience. In the respondent's view, requiring the PSU to undergo CDD measures would dissuade customers from using the services offered by AISPs and PISPs. With regards to Guideline 18.8, 18.10 and 18.12, many respondents argued that the guidelines were not appropriately drafted to take into account the particularities of every PISP business model, and in particular that the guidelines did not take into account PISP business models where the PISP contracts with merchants to offer PIS as a payment alternative for e-commerce transactions. Also, one respondent argued that the requirements regarding CDD measures are outlined in Article 11 of the AMLD, and requested confirmation that therefore guideline 18.8 does not constitute any derogation from Article 11 of the AMLD.	The EBA explicitly acknowledged already in the draft guidelines proposed in the consultation paper that the inherent ML/TF risk associated with AISPs and PISPs is limited and that, in most cases, the low level of inherent risk associated with their business models means that SDD will be the norm. Furthermore, the draft guidelines already differentiated between AISPs' and PISPs' business models and clarified the obligations applicable to each of them, as appropriate. In this context, having assessed the consultation responses, the EBA has added the definitions of Payment Initiation Services and Account Information Services in the PSD2 for further clarification. Also, guideline 18.8 defines the term 'customer' for the purposes of the sector-specific guideline 18. PISPs should assess whether they have a business relationship in the meaning of the AMLD with the payer and/or with the payee, and other circumstances set out in Article 11 AMLD, in order to conclude who the customer is. Consequently, it might be the case that both, the payer and the payee, should be considered customers of the PISP. The EBA acknowledged recently in its Report on the future EU AML/CFT framework (EBA/REP/2020/25), that PISPs do not always enter into a business relationship in the meaning of Article 3(13) of the AMLD with the payer. This may be, for example, the case where the PISP contracts with the payee, to offer PIS as a payment initiation method for e-commerce transactions. In such case, the PISP may not necessarily have a business relationship, in the meaning of the AMLD, with the payer, who might, for example, be using that PISP to make a single or one-off payment to the respective payee. This analysis is without prejudice to	*Guideline 18.1:* *'When applying this Guideline, firms should have regard to the definitions ~~referred to~~ in point 18 and 19 of Article 4 of Directive (EU) 2015/2366 in accordance with which:* *a) a payment initiation service provider (PISP) is a payment service provider pursuing payment initiation services[63] (which in accordance with the definition in point 15 of Article 4 of Directive (EU) 2015/2366 mean services to initiate a payment order at the request of the payment service user with respect to a payment account held at another payment service provider);* *b) an account information service provider (AISP) is a payment service provider offering account information services[64] (which in accordance with the definition in point 16 of*

		Article 11 of AMLD, Title I of these guidelines, and the obligations applicable to PISPs under the PSD2 and other applicable EU legislation. Having assessed the consultation responses, the EBA agrees that additional clarification would be useful and has therefore arrived at the view that, in such cases, the PISP's 'customer' for the purposes of these Guidelines, should be the payee, and not the payer with whom the PISP does not have a business relationship in the meaning of the AMLD. The EBA has therefore amended Guideline 18.8 accordingly. With regards to occasional transactions in the context of PISPs, the EBA recently provided advice to the European Commission (EC) on a future EU AML/CFT framework (EBA/OP/2020/14 and EBA/REP/2020/25), recommending additional clarification.	*Article 4 of Directive (EU) 2015/2366 mean online services to provide consolidated information on one or more payment accounts held by the payment service user with either another payment service provider or with more than one payment service provider).'* *Guideline 18.8* *'The customer is:* *a) For PISPs: the customer is the natural or legal person who holds the payment account and requests the initiation of a payment order from that account ~~(the Payment service user)~~. In the specific case where the PISP has a business relationship in the meaning of Article 3(13) of Directive (EU) 2015/849 with the payee for offering payment initiation services, and not with the payer, and the payer uses the respective PISP to initiate a single or one-off transaction to the respective payee, the PISPs' customer for the purpose of these Guidelines is the payee, and not the payer. This is without prejudice to Article 11 of Directive (EU) 2015/849 and Title I of these guidelines especially with regards to*

			occasional transactions, and the PISPs' obligations under Directive (EU) 2015/2366 and other applicable EU legislation.'
Guideline 18 Guideline 18.4 c) and 18.6 a) Guideline 18.6 b) Guideline 18.7 b)	Several respondents were of the view that the draft guidelines did not reasonably reflect the types and sets of data available for AISPs and PISPs respectively. Several respondents argued that PISPs and AISPs were not able to perform in-depth analyses for AML/CFT purposes and to comply with the requirements under the draft guidelines as their access to information on the related payment transactions was limited. Furthermore, one respondent argued that a consent given by the customer to an AISP was only valid for a maximum of 90 days which limits the ability of AISPs to perform robust transaction monitoring. With regards to Guideline 18.4 c) and 18.6 a), several respondents indicated that AISPs and PISPs did not typically have enough data to be able to determine whether funds, being sent or received from a jurisdiction associated with higher ML/TF risk or a high-risk third country, were suspicious. Also, respondents argued that the term 'known links' in guideline 18.4 c) is equivocal and that every large company with activities in high risk countries could potentially fall under the scope of that guideline. It was suggested to remove this particular reference. With regards to Guideline 18.6 b), one respondent argued that, since the name of the account holder was not always transmitted by ASPSPs to AISPs via the PSD2 interface, it was impossible for an AISP to fulfil the requirement in this guideline. With regards to Guideline 18.7 b), one respondent mentioned that AISPs could access only customer's payment accounts held in an EEA country.	The EBA acknowledges that the amount of information available to AISPs and PISPs will vary depending on several factors, such as their respective service offering and the consent given by the PSU as regards the scope of data AISPs can access. The extent of measures applied by AISPs and PISPs should be risk-based and proportionate to the available data sets. The draft Guidelines proposed in the consultation paper require that AISPs and PISPs take into account all available information. Where data that might be of importance for ML/FT risk assessment purposes is not available to AISPs and PISPs in the context of PSD2, the Guidelines do not require that AISPs and PISPs proactively request such information. Similarly, the draft Guidelines also did not require AISPs or PISPs to proactively research 'someone with known links to those jurisdictions' as referred in guideline 18.4(c). However, having assessed these consultation responses, the EBA agrees that further clarification is warranted and has therefore amended the final guidelines.	*Guideline 18.9:* *'PISPs and AISPs should take adequate measures to identify and assess the ML/TF risk associated with their business. To this end, PISPs and AISPs should take into account all data available to them. The type of data available to them will depend, inter alia, on the specific service offered to the customer, with the explicit consent of the payment service user and which is necessary for the provision of their services, in accordance with Article 66(3), letter (f) and Article 67(2), letter (f) of Directive (EU) 2015/2366.'*
Guideline 18	Several respondents were of the view that the transaction monitoring requirements in the draft Guidelines were	Every obliged entity is responsible to fulfil the requirements under the AMLD. The draft Guidelines, in this context, set clear, reasonable and proportionate requirements on AISPs and PISPs.	*Guideline 18.4:*

Guideline 18.4 Guideline 18.11	disproportionate to the ML/TF risks associated with the provision of AIS and PIS. Also, several respondents argued that transaction monitoring by AISPs and PISPs would create a duplication of the measures already taken by ASPSPs. In these respondents' view, this would contradict the principle of avoidance of repeated procedures, would be disproportionately burdensome, and would lead to delays and inefficiency. With regards to Guideline 18.4 a), several respondents argued that for AISPs offering a balance-only aggregation service, it might not be feasible to perform transaction monitoring at all. Equally, AISPs that have access to a richer data set for the performance of their service might also find it challenging to perform transaction monitoring due to regulatory constraints applicable to their services, such as the requirement for 90 day re-authentication, or the possible revocation of consent by the PSU. Several respondents argued that AISPs would not know the purposes for which each payment account was created, nor would they know the underlying reasons for which the transactions were performed. Moreover, in respondents' view, requirements on transaction monitoring would lead to a large amount of suspicious transactions being reported to FIUs. With regards to Guideline 18.4 b), several respondents argued that a monitoring of the business relationship by AISPs should only be necessary if those AISPs aggregate data from several accounts held by the same customer with more than one ASPSP. With regards to Guideline 18.4 c), one respondent requested confirmation that the requirement in said guideline is applicable to PISPs only with regards to outgoing payments initiated by that PISP, and not for incoming transactions. Several respondents argued that the costs associated with implementing transaction monitoring capabilities could be an overhead that would override the minimal profit margins associated with many AISP business models. Respondents asked the EBA to provide clarity that the level of monitoring undertaken	Article 11 of AMLD provides that it is not necessary to apply CDD measures in every case. However, having assessed the consultation responses, the EBA agrees that further clarifications as regards the requirements applicable to AISPs and PISPs are desirable and has amended the Guidelines. The final Guidelines require that AISPs and PISPs take into account all information available to them in the context of the PSD2, when applying AML/CFT measures, including transaction monitoring. The EBA is aware that there might be situations where service providers do not have the ability to have access to data on single transactions and, consequently, to that extent, are not in a situation to be able to perform transaction monitoring. Aspects of cooperation between ASPSPs and AISPs/PISPs are out of scope of these guidelines and the respondent's suggestion is therefore not being assessed.	*'When assessing ML/TF risks, PISPs and AISPs should take into account at least the following factors as potentially contributing to increased risk:* *a) For PISPs: The customer transfers funds from different payment accounts to the same payee that, together, amount to a large sum without a clear economic or legitimate rationale, or that give the PISP reasonable grounds to suspect that the customer is trying to evade specific monitoring thresholds;* *b) For AISPs: the customer transfers funds from different payment accounts to the same payee, or receives funds on different payments accounts from the same payer, that, together, amount to a large sum without a clear economic or legitimate rationale, or that gives the AISP reasonable grounds to suspect that the customer is trying to evade specific monitoring threshold ~~s using various payment accounts~~;* *~~c) The customer receives funds from, or sends funds to, jurisdictions associated with higher ML/TF risk or to~~*

	by AISPs and PISPs should be risk-based and proportionate to the volume of data held by these providers on their customers. One respondent suggested to clarify in the guidelines that ML/TF detecting would be effective only if PISPs/AISPs actively cooperated with the financial institutions (ASPSP) holding the respective accounts.		~~*someone with known links to those jurisdictions.*~~*'* *Guideline 18.6:* *'When assessing ML/TF risks, PISPs and AISPs should at least take into account the following factors as potentially contributing to increased risk in particular if the customer uses multiple accounts held with different ASPSPs to make payments:* *a) For PISPs: the customer's initiate a payment to a jurisdiction associated with higher ML/TF risk or a high-risk third country or someone with known links to those jurisdictions.* *b) For AISPs: The customer receives funds from, or sends funds to, jurisdictions associated with higher ML/TF risk or a high-risk third country or from/to someone with known links to those jurisdictions, or the customer connects payment accounts held in the name of multiple* ~~*natural or legal*~~ *persons in more than one jurisdiction*~~*; or the customer connects payment accounts in jurisdictions associated with higher ML/TF risks.*~~*'* *Guideline 18.10:*

			'Considering Article 11 of Directive (EU) 2015/849, PISPs and AISPs should determine the extent of CDD measures on a risk-sensitive basis, taking into account all data available to them with the explicit consent of the payment service user and which is necessary for the provision of their services, in accordance with Article 66(3), letter (f) and Article 67(2), letter (f) of Directive (EU) 2015/2366. In most cases, the low level of inherent risk associated with these business models means that SDD will be the norm. With regards to those cases of low risk and to the extent the application of SDD measures is prohibited or restricted under national law, AISPs and PISPs may adjust their CDD measures and apply guideline 18.15 accordingly.' *Guideline 18.11:* *'Monitoring: As part of their CDD processes, PISPs and AISPs should ensure that their AML/CFT systems are set up in a way that alerts them to unusual or suspicious transactional activity, taking into account all data available to them with the explicit consent of the payment*

			service user and which is necessary for the provision of their services, in accordance with Article 66(3), letter (f) and Article 67(2), letter (f) of Directive (EU) 2015/2366. ~~Even without holding significant information on the customer,~~ PISPs and AISPs should use their own, or third party typologies, to detect unusual transactional activity.'
Guideline 18.13	One respondent argued that Article 97 (1) (a) of PSD2 requires Strong Customer Authentication (SCA) to be applied for any access to payment accounts via an AISP and that the identity of the PSU is necessarily established by the ASPSP in a secure and reliable fashion through the application of SCA. This respondent argued that there was therefore no need for additional identity checks by the AISP which, in the respondent's view, cannot produce additional security or transparency. In the same vein, another respondent proposed to delete guideline 18.13 arguing that it was technically not possible for AISPs to verify the validity of the SCA applied by the ASPSP for the PSU to access a particular account. Moreover, this respondent argued that, if AISPs were made aware of the fact that the account was not the customer's own account, but the account of another person (e.g. a relative, or a legal entity), this would not enable a better detection of potential money laundering activities on this account on the basis of an AIS service only. Similarly, another respondent argued that the information required in Guideline 18.13 would not have any impact on the customer's risk qualification by AISPs. There was no higher or lower risk associated with obtaining access to an 'own account', a 'shared account' or one of a 'legal entity'.	The information whether the account is the customer's own account, a shared account, or a legal entity's account to which the customer has a mandate to access (e.g. an association, a corporate account) is relevant for appropriately applying CDD measures. The EBA, having assessed the consultation responses, agrees with the concerns raised and has further clarified this particular guideline. The revised guideline 18.13 now acknowledges that it may also be possible for AISPs to obtain this information through other means. In such a case, an additional information request is not required.	*Guideline 18.13:* *'Pursuant to Article 13(1)(a) of Directive (EU) 2015/849 each time an account is added, the AISP should ask the customer, or verify through other means, whether the account is his own account, a shared account, or a legal entity's account to which the customer has a mandate to access (e.g. an association, a corporate account).'*

Guideline 18.14	One respondent argued that it seemed highly unlikely that EDD measures would be an effective control in mitigating ML risks for AISPs.	The respondent did not provide any rationale for this particular view. The EBA is therefore not in a position to assess the merits of this particular view.	*None*
Guideline 18.15	With regards to Guidelines 18.15 a) and b), one respondent argued that guidance on SDD should not create a form of reliance for AISPs and PISPs on other obliged entities without clarifying the practical implications. In this respondent's view, it was critical to the effectiveness of the overall AML/CFT regime that relying service providers remain ultimately responsible for the CDD. Other respondents were of the view that AISPs should be able to rely on CDD measures performed by the ASPSPs in accordance with the provisions on third party reliance in the AMLD, independent of whether they have a contract with the ASPSP, so as to avoid a duplication of compliance measures. With regards to Guideline 18.15 c), two respondents proposed to clarify the word 'assuming' so that SDD measures do not undermine monitoring for linked transactions and breaches of other SDD thresholds and time limits.	Guidelines 18.15 a) and b) do not amend the principle that AISPs and PISPs are responsible for applying their AML/CFT related measures. Even while applying SDD measures, AISPs and PISPs should perform especially transaction monitoring. In any case, AISPs and PISPs, in accordance with the AMLD and Title I of these Guideline, should ensure that their risk assessments are kept updated. Guideline 18.11 states that PISPs and AISPs should ensure that their AML/CFT systems are set up in a way that alerts them to unusual or suspicious transactional activity.	*None*
Feedback on responses to Question 19 (currency exchanges)			
No comments received	N/A	N/A	*N/A*
Feedback on responses to Question 20 (corporate finance)			
Guidelines 20	One respondent suggested that the EBA should consider issuing 'guidelines on Sovereign Bonds or Sovereign borrowers from highly corrupt countries' to minimize misappropriation, mismanagement and diversion of public funds in developing or highly corrupt countries. The respondent, in this context, discussed several aspects, including in relation to the Covid-19 pandemic.	The respondent's concerns and the background provided do not relate to the new, sector-specific Guidelines 20.	*None*

Guideline 20.1	One respondent suggested to indicate that the activities encompassed in corporate finance were 'M&A' and 'securities issuance', that clients are not only 'corporates' but also sometimes 'institutionals' (e.g. state funds) and more rarely individuals, and that investors in securities issuance should also be taken into account.	Guideline 20.1 as an introduction already covers all relevant cases. However, having assessed the consultation response, the EBA agrees that it could be further clarified that the examples mentioned in the guideline are not exhaustive, and has therefore amended the guideline accordingly.	*'20.1. Firms providing corporate finance services should take into account the inherent ML/TF risks linked with these activities and be mindful that such activity is based on close advisory relationships in particular with corporate clients and other parties such as potential strategic investors.'*
Guideline 20.3 a)	Two respondents suggested another wording ('the ownership structure of the customer is opaque with no reasonable business reason') for more clarity.	Guideline 20.3 mentions risk factors that potentially contribute to an increased risk. Having assessed the consultation responses in the context of other guidelines such as 2.6 d), 4.15 and 9.6 a) vii), the EBA has aligned the wording to make it consistent throughout the Guidelines.	*'20.3 [...] a) the ownership of the customer is opaque without any obvious commercial or lawful rationale. For example, where ownership or control is vested in other entities such as trusts or (Securitisation) special purpose entity~~ies~~ (SSPE).'*
Guideline 20.3 c)	Three respondents suggested to delete the guideline as this was referring to a legal risk. One of those respondents also suggested a different wording ('where the firm has doubts whether the customer has received a mandate or a sufficiently senior management approval to conclude the contract').	Guidelines 20.3 contain risk factors that potentially contribute to an increased risk. This includes the risk that the customer does not act lawfully.	*None*
Guideline 20.3 d)	One respondent asked for clarification and suggested to provide examples of situations that are being addressed.	Guidelines 20.3 contain risk factors that potentially contribute to an increased risk. Guideline 20.3 d) states the risk factor 'where there are few independent means of verification of the customer's identity'. Title I of the Risk Factors Guidelines provides further details on this point.	*None*
Guideline 20.3 e)	One respondent asked for clarification about the clause 'liaison with the authorities is necessary' and questioned whether this meant suspicious transaction reports to FIUs.	Having assessed the consultation response, the EBA agrees that further clarification is reasonable and has therefore amended the Guideline. Guideline 20.3 focuses on risk factors only and does not include any requirements on measures to take.	*'20.3 e) Misconduct such as securities fraud or insider trading is suspected~~: in such case, the assets themselves~~*

			~~could be considered the proceeds of crime and liaison with the authorities is necessary~~.'
Guideline 20.5	One respondent mentioned a typing error as there were two paragraphs 20.5.	The numbering of guideline 20 has been updated accordingly.	*Numbering of 20.5 and following updated.*
Guideline 20.5 a)	Two respondents mentioned that it should be highlighted that this aspect was not always known to the firm and there was no definition of the term 'associated with' which was too broad. Another wording has been suggested as firms were not obliged to identify the address of the beneficial owner nor its relations with jurisdictions associated with higher ML/TF risks which would be a very heavy operational constraint.	Guidelines 20.5 contain country or geographical risk factors that potentially contribute to an increased risk. Title I of the Risk Factors Guidelines provides further details on the requirements concerning jurisdictions associated with higher ML/TF risk.	*None*
Guideline 20.7	One respondent mentioned that the identification of beneficial owners and their links with PEPs was part of the standard CDD and not an enhanced due diligence and that guideline 20.7 a) appears to be redundant with the previous paragraph. This respondent suggested to delete the introductory part of guidelines 20.7.	The EBA, having assessed the consultation response, has amended the introductory part of Guideline 20.7.	*'20.7: Where the risk associated with a business relationship or an occasional transaction is increased, firms should apply EDD measures such as ~~beneficial ownership, and in particular any links the customer might have with politically exposed persons, and the extent to which these links affect the ML/TF risk associated with the business relationship~~:'*
Guideline 20.7 a)	Two respondents mentioned that it was not clear which additional checks on customers' ownerships were expected. Establishing beneficial ownership was a measure that related to CDD, rather than a measure specific to enhanced due diligence. These respondents also argued that the expression 'any links the customer might have with PEP' was unclear.	Guideline 20.7 a) sets out what EDD checks might entail, and complements guidance in Title I of the Risk Factors Guidelines.	*None*

Guideline 20.7 b)	One respondent suggested to clarify that the requirement only covers adverse media screening. Three respondents asked to delete this guideline as (1) the information was not obtained as part of the on-boarding or the customer review, (2) as due diligence on directors was not requested by AMLD and (3) it would be impossible or very difficult to make this assessment.	In high risk situations, it may be appropriate for a firm to consider the integrity of parties that can exercise control over the customer, whether or not they are beneficial owners as defined in Article 3(6) of the AMLD. The sources firms will use to that effect may include, but are not limited to, negative media searches.	*None*
Guideline 20.7 c)	Two respondents asked for clarification what is meant by 'other owners'. Two other respondent suggested to delete the guideline as it seemed disproportionate and constituted a significant operational burden that was not based on provisions from AMLD.	In high risk situations, verification of the identity of owners and controllers other than the beneficial owner as defined in Article 3(6) of the AMLD may help to obtain a clearer picture of the risk associated with the business relationship.	*None*
Guideline 20.7 e)	Three respondents asked for clarification what is meant by 'Establishing the financial situation of the corporate client'. Two respondents asked to delete the guideline as financial institutions regularly assessed the financial situation of the corporate client as part of CDD measures; however, those documents should not be part of the CDD documentation.	The EBA, having assessed the consultation responses, agrees that the Guideline can be further clarified in order to emphasise that there should be 'additional' checks on top of the standard CDD measures. The EBA has amended the Guideline accordingly.	*'20.7 e): Additional checks in order to establish~~ing~~ the financial situation of the corporate client.'*
Guideline 20.7 f)	One respondent mentioned that, in practice, there was no firm using 'non-documentary forms of evidence' due to rules of professional secrecy. It was suggested to delete the guideline. One respondent asked for clarification who the relevant individual is, how credible persons are identified and what their responsibilities could be.	Non-documentary evidence that might not be relevant in each case can contribute to the firm's understanding of its customer. The Guideline is clear that it does not replace standard CDD or EDD measures and is instead complementary.	*None*
Guideline 20.7 g)	One respondent suggested to only require firms to get an understanding of who these parties are and their role, as well as subject these parties to sanctions screening. One respondent asked for more details on the checks to be performed and argued that it was clear that these counterparties are not clients.	The guidelines are clear that additional checks are designed to help the firm to understand the nature of the transaction. The extent of these checks, and the decision whether or not they are appropriate, can be determined on a risk-sensitive basis.	*None*
Guideline 20.7 h)	One respondent mentioned that EDD monitoring for Corporate Finance was typically undertaken manually by the staff engaged in the activity as part of the deal management process and not via the use of automated transaction monitoring systems.	Guideline 20.7 h) does not only cover 'automated transaction monitoring'. As stated by the respondent, firms may use other approaches.	*None*

Guideline 20.7 i)	Two respondents suggested to replace 'confirming' by 'assessing'. One respondent added that reputational risk was not related to financial crime risk and should be managed by individual firms.	The term 'confirming' implies that an assessment and a subsequent verification of the information obtained is necessary. The guideline therefore goes further than a mere assessment. Equally, the EBA, having assessed the consultation responses, agrees with the comment on the reputational risk and, and has amended the guideline accordingly.	*20.7 i): When taking part in securities' issuance, the firm should ~~seek to protect its own reputation by confirming~~ confirm that third-parties participating in selling securitisation instruments or transactions to investors have sufficient customer due diligence arrangements of their own in place.'*

Commission de Surveillance du Secteur Financier
283, route d'Arlon
L-2991 Luxembourg (+352) 26 25 1-1
direction@cssf.lu
www.cssf.lu