EBA/CP/2023/11

31 May 2023

Consultation Paper

Guidelines amending Guidelines EBA/2021/02 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. Responding to this consultation 3

2. Executive Summary 4

3. Background and rationale 6

3.1. Background 6
3.2. Rationale 6
3.3. Scope of the consultation 10

4. Draft Guidelines amending Guidelines EBA/2021/02 11

5. Accompanying documents 34

5.1 Cost-benefit analysis / Impact assessment 34
5.2 Overview of questions for consultation 37

1. Responding to this consultation

The EBA invites comments on all proposals put forward in this paper and in particular on the specific questions summarised in 6.2.

Comments are most helpful if they:

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

Submission of responses

To submit your comments, click on the 'send your comments' button on the consultation page by 31.08.2023. Please note that comments submitted after this deadline, or submitted via other means may not be processed.

Publication of responses

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

Data protection

The protection of individuals with regard to the processing of personal data by the EBA is based on Regulation (EU) 1725/2018 of the European Parliament and of the Council of 23 October 2018. Further information on data protection can be found under the legal notice section of the EBA website.

2. Executive Summary

In July 2021, the European Commission issued a legislative package with four proposals to reform the EU's legal and institutional anti-money laundering and countering the financing of terrorism (AML/CFT) framework. The legislative package included a proposal for a recast of Regulation (EU) 2015/847 on information accompanying transfers of funds and repealing Regulation (EC) No 1781/2006 (FTR). According to the 'Provisional Agreement Resulting from Interinstitutional Negotiations' of 5 October 2022 (2021/0241 (COD)) (hereafter 'Provisional Agreement') the co-legislators intended to extend the scope of Regulation (EU) YYYY/XX [to insert FTR reference once published] to transfers of crypto assets. It also amends Directive (EU) 2015/849 to subject crypto-asset service providers to the same AML/CFT requirements and AML/CFT supervision as credit and financial institutions.

With this change and given that the EBA's Guidelines (EBA/GL/2021/02) 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 apply to credit and financial institutions under that Directive, the scope of the guidelines is automatically extended.

Article 38 of the Regulation (EU) YYYY/XX [to insert FTR reference once published] mandates the EBA to issue guidelines on the risk variables and risk factors crypto assets service providers (CASPs) should take into account when entering into a business relationship or carrying out transactions in crypto assets. In preparation of the upcoming mandate, the EBA is proposing to amend the ML/TF Risk Factors Guidelines.

The amending guidelines:

- highlight specific risk factors in Title I, that reflect specific features of crypto assets and CASPs and which should be considered by credit and financial institutions when entering into a business relationship or correspondent relationship with CASPs;
- emphasise the need for secure remote onboarding tools to be put in place by credit and financial institutions;
- provide further guidance for credit and financial institutions when entering into business relationships with service providers in crypto assets ecosystem established in a third country, that are not regulated under Regulation (EU) YYYY/XX [to insert MiCA reference once published] or under any other relevant EU regulatory framework;

- provide new sector-specific guidance for CASPs in Title II of the ML/TF Risk Factors Guidelines (Guideline 21), explaining the risk increasing and reducing factors that CASPs should consider when assessing risks associated with their customer business relationships. In addition to cross-sectoral risk factors relevant in all sectors, the guidelines emphasise the risks for CASPs that are associated with:

    - transactions, such as transactions with self-hosted addresses or with service providers in a crypto assets ecosystem established in a third country that are not regulated under the MiCA Regulation or under any other relevant regulatory framework within or outside the EU;

    - products, such as those containing privacy-enhancing features or allowing the use of cash and crypto-ATMs when exchanging crypto assets to fiat currencies;

    - the nature of customers and their behaviour, for example, customers who use IP addresses that are linked to darknet or customers that are involved in crypto mining in high-risk jurisdictions;

    - the customers' or beneficial owners' links to high-risk jurisdictions or transactions to/from jurisdictions associated with high risk of ML/TF, including the location of crypto-ATMs in those jurisdictions.

- provide guidance on mitigating measures CASPs should apply in situations where the risk is either increased or reduced.

Next steps

The draft amending guidelines are published for a 3-months public consultation. The EBA will finalise these guidelines once the consultation responses have been assessed.

3. Background and rationale

3.1. Background

1. In July 2021 the European Commission issued a legislative package with four proposals to reform the EU's legal and institutional anti-money laundering and countering the financing of terrorism (AML/CFT) framework. The legislative package included a proposal for a recast of Regulation (EU) 2015/847[1].

2. This recast extends the scope of Regulation (EU) 2015/847 to transfers of crypto assets. It also extends the definition of 'financial institution' in Directive (EU) 2015/849[2] to CASPs that are regulated in accordance with Regulation (EU) [xxxx/xxx][3] (the 'MiCA Regulation'). CASPs as defined in the MiCA Regulation will be subject to the same AML/CFT systems and controls requirements as credit and financial institutions.

3. Article 38 of the recast Regulation (EU) 2015/847 amends Article 18 of the Directive (EU) 2015/849 and mandates the EBA to issue guidelines on the risk variables and risk factors CASPs should take into account when entering into a business relationship or carrying out transactions in crypto assets. In particular, it requires the EBA to clarify the enhanced due diligence requirements CASPs should apply in high-risk situations, and the mitigating measures CASPs should apply when entering into similar correspondent relationships[4], particularly with entities that are not covered by Directive (EU) 2015/849.

4. To fulfill this mandate, the EBA is proposing to amend the EBA's Guidelines (EBA/2021/02) 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 under Articles 17 and 18(4) of Directive (EU) 2015/849 (the 'ML/TF Risk Factors Guidelines').

3.2. Rationale

5. The EBA performed an analysis of the ML/TF Risk Factors Guidelines to establish whether new, or amended guidelines were necessary to fulfil this mandate.

[1] 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 (OJ L 141 5.6.2015, p. 1)

[2] 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/EC (OJ L 141 5.6.2015, p. 73-117)

[3] Insert reference number when available

[4] Article 38.2(b) of the recast Regulation (EU) 2015/847

6. The EBA concluded that the general approach to identifying and assessing ML/TF risk associated with credit and financial institutions' business or their business relationships with customers and the application of adequate customer due diligence ('CDD') measures set out in Title I of these guidelines should apply to CASPs as it does to other financial institutions. It also concluded that several provisions in Title I and Title II of these Guidelines would benefit from clarification to reflect the specific features of crypto assets and the nature of CASPs' business models to envisage the impact these may have on CASPs' exposure to ML/TF risk.

7. The EBA therefore proposes to amend specific provisions in Title I and Title II of these Guidelines. It also proposes to include new sectoral guidelines that are specific to CASPs in Title II of these guidelines.

8. This section explains the rationale for the amending ML/TF Risk Factors Guidelines.

Amendments to Subject matter, scope and definitions

9. The amended Guidelines provide clarification that the definitions as set out in Directive (EU) 2015/849 and Regulation (EU) 2015/847 (recast) apply also in these guidelines. The terms, that have been defined in the legislation, have been removed from the list of definitions.

Question 1: Do you have any comments on the proposed changes to definitions?

Amendments to Guideline 1: Risk assessments: key principles for all firms

10. The Guideline sets out general principles that credit and financial institutions, which are defined in the Guidelines as 'firms', need to apply when carrying out an assessment of ML/TF risks associated with their business and individual business relationships. These principles apply to CASPs as they do to other firms. Proposed amendments to Guideline 1.7 recognise that vulnerabilities in credit and financial institutions' systems and controls framework may expose them to ML/TF risks and specify that firms should carry out a ML/TF risk assessment before launching new practices, products or services.

Question 2: Do you have any comments on the proposed changes to Guideline 1?

Amendments to Guideline 2: Identifying ML/TF risk factors

11. This guideline sets out different risk factors associated with customers, products, delivery channels and geographies that firms should consider when carrying out their assessment of risks. Proposed amendments to Guideline 2.4 provide that firms should consider whether their customers' business activities involving crypto assets may expose these firms to increased ML/TF risk.

Question 3: Do you have any comments on the proposed changes to Guideline 2?

Amendments to Guideline 4: CDD measures to be applied by all firms

12. This guideline explains the key considerations firms should apply when adjusting CDD measures based on the risk profile of the customer, and the steps they should take to keep CDD measures up to date. Considering that most CASPs onboard their customers remotely using innovative solutions, the proposed amendments highlight the need for CASPs and other firms also using innovative solutions to ensure compliance with the EBA's Guidelines (EBA/GL/2022/15) on the use of Remote Customer Onboarding Solutions.

13. Guideline 4.60 was amended to reflect some of the red flag indicators related to CASPs that were highlighted by the Financial Action Task Force in 2020. The proposed amendments recognise that transactions that are more frequent than usual or transactions involving small amounts that are unusually frequent, or successive transactions without obvious economic rationale may be indicators of unusual transactions. In addition, proposed amendments to Guideline 4.74 emphasise the need for adequate transaction monitoring systems to be put in place by firms and specify that, in some circumstances, advanced analytics tools might be warranted due to the level of ML/TF risks.

Question 4: Do you have any comments on the proposed changes to Guideline 4?

Amendments to Guideline 6: Training

14. Guideline 6 specifies that firms should provide adequate training to their staff. Amended Guideline 6.2 highlights the need for some staff to undergo training of a more technical nature to ensure that they are able to interpret the outcomes of the monitoring systems used by the firm, in particular where advanced analytics tools are used.

Question 5: Do you have any comments on the proposed changes to Guideline 6?

Amendments to Guideline 8: Sectoral guideline for correspondent relationships

15. In this guideline, the EBA provides guidance to firms that are offering correspondent relationship services. They explain how firms should identify risks associated with respondents and set out the type of CDD measures they should apply to mitigate these risks. These guidelines will also apply to CASPs[5].

16. Amended Guideline 8 specifies the risk to be considered and the measures to be applied by firms where the respondent is a CASP; or the respondent's customers are CASPs; or where the respondent or its customers are providers of services in crypto-assets ecosystems established in third countries that are not regulated under the MiCA Regulation or under any other relevant EU regulatory framework and, that are bound by AML/CFT regulatory and supervisory regime, that is less robust than the regime foreseen in Directive (EU) 2015/849.

Question 6: Do you have any comments on the proposed changes to Guideline 8?

[5] Article 38.2(b) of the recast Regulation (EU) 2015/847

Amendments to Guideline 9: Sectoral guideline for retail banks

17. Proposed amendments to these guidelines recognise that, as a result of changes in the legislative framework introduced by the MiCA Regulation, CASPs will be engaging increasingly with, or be customers of banks. They make clear that banks should be mindful that some providers of crypto asset services remain outside the scope of the regulatory and supervisory framework in the EU or abroad, including AML/CFT framework and therefore may present increased ML/TF risks. Proposed amendments also clarify that CASPs should also consider guideline 21.

Question 7: Do you have any comments on the proposed changes to Guideline 9?

Amendments to Guideline 10 and Guideline 15 and Guideline 17

18. These are guidelines addressed to firms in different sectors. Proposed amendments clarify that CASPs should also consider Guideline 21.

19. In Guideline 17, proposed amendments replace references to 'virtual currencies' with references to 'crypto assets'.

Question 8: Do you have any comments on the proposed changes to Guidelines 10, 15 and 17?

Guideline 21: Sectoral guideline for crypto asset services providers (CASPs)

20. Guideline 21 is new. Like other guidelines in Title II, it should be read in conjunction with Title I that apply to all firms. The EBA proposes to add it to the guidelines to clarify regulatory expectations for CASPs when they identify and assess ML/TF risk associated with their overall business and with individual business relationships. In particular, the amending guideline acknowledges that transactions with self-hosted addresses and the products or services offered by CASPs that entail privacy-enhancing features or offer a higher degree of anonymity may expose them to increased ML/TF risk. Also, the global nature of CASPs' business models may present heightened ML/TF risks, particularly where CASPs' customers are transacting with jurisdictions associated with a high risk of ML/TF.

21. Guideline 21 also sets out enhanced and simplified CDD measures that CASPs should apply to business relationships, which are exposed to increased or low risk of ML/TF. In most cases, CDD measures applied by CASPs are similar to or the same as those applied by other firms, but some differences exist. This is the case in particular with regard to the monitoring of customers and their transactions, where the draft amending guidelines require that CASPs should have adequate procedures and systems in place to monitor all types of crypto assets. CASPs should also determine circumstances when the use of advanced analytics tools is warranted for their business.

Question 9: Do you have any comments on the proposed changes to Guideline 21?

3.3. Scope of the consultation

22. The scope of the consultation, and of the consultation questions, is limited to the proposed amendments. Comments on other aspects of the ML/TF Risk Factors Guidelines will not be considered.

23. The draft amending guidelines are published for a three-months public consultation.

4. Draft Guidelines amending Guidelines EBA/2021/02

EBA/GL/20XX/XX

DD Month YYYY

Draft Guidelines amending Guidelines EBA/GL/2021/02

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

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[6]. 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 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 primarily directed at institutions.

Reporting requirements

3. According to Article 16(3) of Regulation (EU) No 1093/2010, competent authorities must notify the EBA as to whether they comply or intend to comply with these guidelines, or otherwise with reasons for non-compliance, by [dd.mm.yyyy]. 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 with the reference 'EBA/GL/2023/xx'. 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 EBA.

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

[6] 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

Addressees

5. These guidelines are addressed to credit and financial institutions as defined in Article 3(1) and 3(2) of Directive (EU) 2015/849[7] and to competent authorities as defined in Article 4(2) point (iii) of Regulation (EU) 1093/2010.

[7] 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 (OJ L 141, 5.6.2015, p 73-117)

3. Implementation

Date of application

6. These guidelines apply 6 months after the date of publication on the EBA's website of the guidelines in all EU official languages.

4. Amendments

(i) Amendments to Subject matter, scope and definitions

7. Paragraph 12 is amended by replacing the introductory sentence with the following sentence: 'Unless otherwise specified, terms used and defined in Directive (EU) 2015/849 and Regulation (EU) XXXX/XXX[8] have the same meaning in the guidelines. In addition, for the purposes of these guidelines, the following definitions apply:'

8. Paragraph 12 point (f) and (m) are deleted.

(ii) Amendments to Guideline 1: Risk assessments: key principles for all firms

9. At the end of Guideline 1.7 the following new letter is added:

'd) Where the firm is launching a new product or service, or a new business practice, including a new delivery mechanism, or is adopting an innovative technology as part of its AML/CFT systems and controls framework, it should assess the ML/TF risk exposure prior to the launch and reflect this assessment in the firm's business-wide risk assessment and its policies and procedures.'

(iii) Amendments to Guideline 2: Identifying ML/TF risk factors

10. Guideline 2.4 letter b) is amended as follows:

'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, unregulated businesses that provide services related to crypto assets as described in Guideline 9.21, casinos or dealers in precious metals?'

(iv) Amendments to Guideline 4: CDD measures to be applied by all firms

11. The introductory sentence of Guideline 4.29 is amended as follows:

'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 in accordance with the EBA's Guidelines (EBA/GL/2022/15) on the use of Remote Customer Onboarding Solutions under

[8] Reference to be inserted to the recast FTR

Article 13(1) of Directive (EU) 2015/849, firms should:'

12. Guideline 4.35 is amended as follows:

'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. The firm should also ensure that it can promptly access the relevant customer data and information when necessary.'

13. Guideline 4.60 letter a) is amended as follows:

'a) they differ from what the firm would normally expect, including when transactions are larger or more frequent than usual or transactions involving small amounts that are unusually frequent, or there are successive transactions without obvious economic rationale.'

14. Guideline 4.61 letter a) is amended as follows:

'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 crypto assets or finding out more about the customer's business to ascertain the likelihood of the customer making such transactions; and'

15. Guideline 4.74 letter b) is amended as follows:

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

16. In Guideline 4.74 a new letter is added as follows:

'd) whether the use of advanced analytics tools, like the distributed ledger analytics tools, is necessary in light of the ML/TF risk associated with the firm's business, and with the firm's customers' individual transactions.'

(v) Amendments to Guideline 6: Training

17. Guideline 6.2 letter c) is amended as follows:

'c) How to recognise suspicious or unusual transactions and activities, taking into account the specific nature of their products and services, and how to proceed in such cases;'

18. In Guideline 6.2 a new letter is added as follows:

‘d) How to use automated systems, including advanced analytics tools, to monitor transactions and business relationships, and how to interpret the outcomes from these systems and tools.’

(vi) Amendments to Guideline 8: Sectoral guideline for correspondent relationships

19. Guideline 8.6 letter d) is amended as follows:

‘d) The respondent conducts significant business with sectors that are associated with higher levels of ML/TF risk; for example, the respondent conducts:

i. significant remittance business;
ii. business on behalf of certain money remitters or exchange houses;
iii. business on behalf of or with providers of services in the crypto-assets ecosystem established in third countries which are not regulated under Regulation (EU) XXXX/XXX[9] or under any other relevant EU regulatory framework and which are bound by an AML/CFT regulatory and supervisory regime that is less robust than the regime foreseen in Directive (EU) 2015/849;
iv. business on behalf of CASPs which allow transfers to and from self-hosted addresses;
v. business with non-residents or
vi. business in a currency other than that of the country in which it is based.

20. In Guideline 8.6 a new letter is added as follows:

‘h) the ownership of the IBAN account provided by a respondent CASP to receive fiat funds from customers is in the name of a company other than the CASP.’

21. In Guideline 8.8 a new letter is inserted as follows:

‘d) The respondent is unable to verify with a sufficient level of certainty that its customers are not based in jurisdictions stated in point a) of Guideline 8.8, including when the respondent is unable to verify the IP addresses of its customers, in circumstances where it is required by the respondent’s policies and procedures.’

22. Guideline 8.17 letters a) and c) are amended as follows:

‘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

[9] Insert reference number for the MiCA Regulation when available.

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 or, if relevant, the type of crypto assets the respondent CASP will transact through the correspondent account.'

'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 include the transaction monitoring tools in place to ensure that they are adequate for the type of business carried out by the respondent. 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.'

(vii) Amendments to Guideline 9: Sectoral guideline for retail banks

23. Guideline 9.3 is amended as follows:

'9.3. Banks should consider the following risk factors and measures alongside those set out in Title I of these guidelines. Banks that provide wealth management services should also refer to sectoral guideline 12, payment initiation services or account information services should also refer to the sectoral guideline 18 and those that provide crypto asset services should refer to the sectoral guideline 21.'

24. Guideline 9.16 is amended as follows:

'9.16 Where a bank's customer opens a 'pooled/ omnibus account' in order to administer funds or crypto assets 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.'

25. Guideline 9.17 is amended as follows:

'9.17 Where a bank has determined, based on its ML/TF risk assessment carried out in accordance with these guidelines, that the level of the ML/TF risk associated with the business relationship is high, it should apply the EDD measures set out in Article 18 of Directive (EU) 2015/849 as appropriate.'

26. The introductory sentence of Guideline 9.18 is amended as follows:

'9.18. However, to the extent permitted by national legislation, where, in accordance with the

individual ML/TF risk assessment of the customer, the risk associated with the business relationship is low, a bank may apply SDD measures, provided that:'

27. The heading of Guidelines 9.20 to 9.24 is amended as follows:

'Customers that offer services related to crypto-assets'

28. Guidelines 9.20 to 9.23 are replaced as follows:

'9.20 When entering into a business relationship with a customer who is a provider of services in a crypto-assets ecosystem established in a third country, which is not regulated under Regulation (EU) [xxxx/xxx][10] or under any other relevant EU regulatory framework, banks may be exposed to increased risk of ML/TF. Banks should carry out the ML/TF risk assessment of these customers and, as part of this, banks should also consider the ML/TF risk associated with the specific type of crypto assets.

9.21 To ensure that the level of ML/TF risk associated with customers described in Guideline 9.20 is mitigated, banks, as part of their CDD measures, should at least:

a) enter into a dialogue with the customer to understand the nature of the business and the ML/TF risks to which it is exposed;

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 EU/EEA Member state or a third country, and, in the case of a third country, take a view on the adequacy of that third country's AML/CFT regulatory and supervisory regime;

e) establish whether the services provided by the customer fall within the scope of the registration or licence of the customer;

f) establish whether the customer is providing other services for which it is registered or licensed as a credit or financial institution;

g) find out whether businesses issuing crypto assets to raise funds such as Initial

[10] Insert reference number for the MiCA Regulation when available.

Coin Offerings (ICOs), are legitimate and, where applicable, regulated for AML/CFT purposes in accordance with internationally agreed standards, such as standards published by the Financial Action Task Force.'

(viii) Amendments to Guideline 10: Sectoral guideline for electronic money issuers

29. Guideline 10.2 is amended as follows:

'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 should also refer to the sectoral guideline 18. The sectoral guideline 11 for money remitters may also be relevant in this context. Firms that provide crypto asset services should also refer to the sectoral guideline 21'.'

(ix) Amendments to Guideline 15: Sectoral guideline for investment firms

30. Guideline 15.1 is amended as follows:

'15.1. Investment firms as defined in point (1) of Article 4(1) of Directive 2014/65/EU should 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 guidelines 12 and 21 may also be relevant in this context.'

(x) Amendments to Guideline 17 Sectoral guideline for regulated crowdfunding platforms

31. Guideline 17.4 letter i) is amended as follows:

' i). The CSP allows payments through the crowdfunding platform in crypto assets.'

32. Guideline 17.6 letter b) is amended as follows:

'b) The investor or the project owner transfer crypto assets.'

33. After Guideline 20, a new Guideline 21 is inserted as follows:

(xi) 'Guideline 21: Sectoral guideline for crypto asset services providers (CASPs)

21.1. CASPs should be mindful that they are exposed to ML/TF risks due to specific features of their business model and technology used as part of their business which allows them to transfer crypto assets instantly across the world and onboard customers in different jurisdictions. The risk is further increased when they process or facilitate transactions or offer products or services which contain privacy-enhancing features or which offer a higher degree of anonymity.

21.2. When offering crypto asset services, CASPs should comply with provisions in Title I as well as the provisions set out in this sectoral guideline and Guideline 8, if relevant.

Risk factors

Product, services and transaction risk factors

21.3. The following factors may contribute to **increasing risk**:

a) the products or services offered by CASPs entail privacy-enhancing features or offer a higher degree of anonymity such as, but not limited to, mixers or tumblers, obfuscated ledger technology, Internet Protocol (IP) anonymizers, ring signatures, stealth addresses, ring confidential transactions, atomic swaps, non-interactive zero-knowledge proofs and so-called privacy coins;

b) the product allows payments from third parties that are neither associated with the product nor identified upfront, where such payments have no apparent economic sense;

c) the product places no restrictions on the overall volume or value of transactions;

d) the product allows transactions between the customer's account and:

i. self-hosted addresses;

ii. crypto-asset accounts or distributed ledger addresses managed by a provider of services in crypto-assets ecosystem which is not regulated under EU law and which is not regulated under any other laws similar to Regulation (EU) XXXX/XXX[11], or which is subject to the AML/CFT regulatory and supervisory regime that is less robust than the regime foreseen in Directive (EU) 2015/849

iii. crypto-asset accounts or distributed ledger addresses managed by a provider of services in a crypto-assets ecosystem established in a third country, which is not regulated under Regulation (EU)

[11] Insert reference number for the MiCA Regulation when available.

XXXX/XXX[12] or under any other EU relevant regulatory framework, and which is subject to the AML/CFT regulatory and supervisory regime that is less robust than the regime foreseen in Directive (EU) 2015/849

iv. a peer-to-peer cryptocurrency exchange platform or a mixer or a tumbler platform;

v. crypto-assets' decentralized or distributed application, which is not controlled or influenced by a legal or natural person (often referred to as 'decentralised finance' (DeFi));

vi. crypto-ATMs or other hardware that involves the use of cash or electronic money, that benefits from exemptions under Article 12 of Directive (EU) 2015/849 or that does not fall within the regulatory and supervisory regime in the EU.

e) products involving new business practices, including new delivery mechanisms, and the use of technologies where the level of the ML/TF risk is not yet fully understood by the CASP;

f) where the CASP is offering nested services (a service within a service) of a wholesale CASP where the wholesale CASP exercises only weak control over the nested service;

21.4. The following factors may contribute to **reducing risk:**

a) products with reduced functionality, such as low transaction volumes or values;

b) the product permits transactions between the customer's account and

i. crypto-asset accounts or distributed ledger addresses in the customer's name held by the CASP;

ii. a crypto asset account or distributed ledger address in the customer's name, that is held by a service provider in crypto assets ecosystem, which is regulated outside the EU under the regulatory framework, that is as robust as that foreseen in Regulation (EU) XXXX/XXX[13] and which is subject to AML/CTF regulatory and supervisory framework that is as robust as the one provided for in Directive (EU) 2015/849; or

iii. a bank account in the customer's name at a credit institution that is

[12] Insert reference number for the MiCA Regulation when available.

[13] Insert reference number for the MiCA Regulation when available.

subject to AML/CFT regulatory and supervisory framework set out in Directive (EU) 2015/849 or another legislative framework outside the EU that is as robust as the one provided for in Directive (EU) 2015/849.

c) the nature and scope of the payment channels or systems used by the CASP is limited to closed-loop systems or systems intended to facilitate micro-payments or government-to-person or person-to-government payments;

d) the product is available only to certain categories of customers, like employees of a company that has issued a crypto asset;

Customer risk factors

21.5. The following factors may contribute to **increasing risk:**

a) regarding the **nature of the customer** in particular:

i. a non-profit organisation that has been linked, on a basis of reliable and independent sources, to extremism, extremist propaganda or terrorist sympathies and activities, or has been involved in misconduct or criminal activities, including ML/TF or corruption related cases.
ii. an undertaking that is a shell company,
iii. a company, which has been recently established and is processing large volumes of transactions,
iv. a shelf company, which despite being established for some time only recently became active and started processing large volumes of transactions;
v. an undertaking, which is in an intra-group relationship with other crypto-asset businesses;
vi. an undertaking or a person who is using an IP address associated with a darknet or other similar software that allows anonymous communication, including encrypted emails and VPNs.
vii. a vulnerable person or a person who displays very little knowledge and understanding of crypto assets or the related technology, which may increase the risk that the customer is being used as a money mule;

b) regarding the **customer's behaviour,** situations where the customer

i. tries to open multiple crypto asset accounts with the CASP;

ii. or the customer's beneficial owner is unable or unwilling to provide the necessary CDD information, without any legitimate reason for it, by:
   a) deliberately avoiding direct contact, either in person or via remote onboarding tools;
   b) trying to obscure the beneficial owner of the funds through the engagement of agents or associates, such as providers or trust services or corporate services, in the business relationship or transactions;
   c) remaining silent or trying to mislead the CASP about the source of funds or the source of crypto assets used to purchase crypto assets or the purpose of the transactions.

iii. uses an IP address or mobile device that is linked to multiple customers, without any apparent economic reason, or that is known to be linked to potentially illegal or criminal activities; or the customer's crypto asset account is accessed from multiple IP addresses without any evident link to the customer;

iv. provides information that is inconsistent, including when the customer's IP address is inconsistent with other information about the customer, like the information obtained in accordance with Article 14(1) and 14(2) of Regulation (EU) 2015/847 (recast), or the customer's given country of residence, registration or business activities (both at the time of entry into the business relationship and at the time of the transaction), the information about the sources of funds or the source of crypto assets is inconsistent with other CDD information or the customer's overall profile.

v. appears to belong to a group of individuals that conduct their transactions at single or multiple outlet or locations or across multiple services;

vi. frequently changes its personal information or its payment instruments without obvious reason, including frequent changes of an account number or a payment card number.

vii. appears to persistently avoid CDD requirements by transferring amounts of crypto assets that are just below the threshold defined in Article 14(5) and Article 16(2) of Regulation (EU) 2015/847 (recast);

viii. indicates that the purpose is to invest in an ICO or in a crypto asset/product offering a high return or to invest in a crypto asset which is not supported by a white paper required under the Regulation (EU) xxxx/xxx[14].

[14] Insert reference to the MiCA Regulation

ix. displays behaviour or the customer's transaction volume or pattern is not in line with that expected from the type of customer or the risk category to which it belongs, or is unexpected based on the information the customer provided to the CASP, either at the start or throughout the business relationship. Such circumstances include the customer:
   a) unexpectedly and without obvious reason significantly increasing the volume or value of a crypto asset transfer or combined transfers after a period of dormancy;
   b) transacting with an unusually high frequency, volume or value of crypto assets, which is inconsistent with the purpose and nature of the business relationship and without an apparent economic purpose;
   c) increasing the transaction limit shortly after having established a business relationship with the CASP;

x. displays behaviour, which is unusual because it involves transfers to/from distributed ledger addresses in multiple jurisdictions or transfers crypto assets with no apparent business or lawful purpose;

xi. when exchanging crypto assets to fiat currencies and vice versa, the customer:
   a) uses multiple bank or payment accounts, credit cards or prepaid cards to fund the crypto assets account;
   b) uses a bank or payment account, credit card in the name of a different person than the customer without having evident links to that person;
   c) uses a bank or payment account located in a jurisdiction, which is inconsistent with the customer's given address or location;
   d) uses multiple Payment Solutions Providers (PSP);
   e) repeatedly requests an exchange to or from cash, privacy coins or anonymous electronic money;
   f) uses bridges to change crypto asset to privacy crypto assets, such as Monero, Zcash or similar;
   g) uses Crypto-ATMs in different locations to repeatedly transfer funds to a bank account.

xii. is investing or exchanging crypto assets, which it has borrowed via a peer-to-peer or other lending platform that does not fall within the scope of Regulation (EU) XXXX/ XXX[15] or under any other relevant regulatory framework within or outside the EU and, which is notably a decentralized or distributed application with no legal or natural person with control or influence over it.

[15] Insert reference to MiCA ReEgulation

xiii. directly or indirectly receives or sends crypto assets related ML/TF or related criminal activities previously identified as such.

xiv. is investing or exchanging crypto assets, which themselves entail privacy-enhancing features or offer a higher degree of anonymity (such as privacy coins) or the customer receives crypto assets which have been subject to privacy-enhancing activities, in particular processes which obfuscate the transaction on the ledger technology or contain other characteristics similar to those listed in point a) of guideline 21.5.

xv. repeatedly receives crypto assets from or sends crypto assets to:

a) a crypto asset account through an intermediary service provider, which does not fall within the scope of Regulation (EU) XXXX/ XXX[16] or under any other relevant regulatory framework within or outside the EU; or which is subject to AML/CTF regulatory and supervisory framework that is less robust than the one provided for in Directive (EU) 2015/849;

b) multiple self-hosted addresses or multiple addresses located in other CASPs;

c) a newly created crypto asset account or a distributed ledger address held by a third party;

d) self-hosted addresses on decentralised platforms, which involve the use of mixers, tumblers and other privacy enhancing technologies that may obfuscate the financial history associated with the distributed ledger address and the source of funds for the transaction, therefore undermining the CASP's ability to know its customers and implement effective AML/CTF systems and controls;

e) a crypto asset account shortly after being onboarded by the CASP, which is then followed by a withdrawal from the customer's account in a short period of time;

f) a crypto asset account frequently below a defined threshold or, in case of transfers to a self-hosted address, under the threshold of EUR 1 000 as defined in Article 14(5) and Article 16(2) of the Regulation (EU) 2015/847 (recast);

g) a crypto asset account by splitting the transactions in a multiple of transactions which are sent to multiple distributed ledger addresses by using smurfing techniques;

xvi. The customer exploits technological glitches or failures to his advantage.

[16] Insert reference to MiCA R~~e~~egulation

21.6. The following factors may contribute to **reducing risk** where the customer:

a) has complied with the travel rule requirements provided for in Regulation (EU) xxxx/xxx[17] during previous transactions in crypto assets and has provided information that allows the identification of a customer or the possibility to check it in case of doubts or suspicion.

b) is well known to the CASP through previous business relationships and the customer's previous transactions in crypto assets have not given rise to suspicion or concern, and the product or service sought is in line with the customer's risk profile.

c) requests an exchange to/ from fiat currency and either the source of or destination of funds is the customer's own bank account with a credit institution in a jurisdiction assessed by the CASP as low risk.

d) requests an exchange and either the source of or destination for the crypto asset is the customer's own crypto asset account or a distributed ledger address hosted by a CASP or by a provider of services in crypto assets ecosystem, which is regulated and supervised outside the EU under a regulatory framework that is as robust as that foreseen in Regulation (EU) XXXX/XXX[18] and, which is subject to AML/CFT requirements as robust as those foreseen in Directive (EU) 2015/849, that has been whitelisted or otherwise determined by the CASP as low-risk.

e) requests an exchange and either the source of or destination for the crypto asset relates to low value payments for goods and services to/ from a lawful merchants or service providers.

Country or geographical risk factors

21.7. The following factors may contribute to **increasing risk:**

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

b) The originating or the beneficiary crypto asset account or a distributed ledger address is linked to a jurisdiction:

i. which is associated with a weak AML/CFT regime, meaning that the AML/CFT regulatory and supervisory regime in that jurisdiction is less robust than the regime foreseen in Directive (EU) 2015/849.

[17] A reference to the FTR recast to be inserted

[18] Insert reference to the MiCA Regulation when available.

ii. associated with higher ML/TF risk or jurisdictions/regions 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.

c) The customer or the customer's beneficial owner is a resident, is established, operates in or has links with a jurisdiction associated with an increased ML or TF risk.

d) The business relationship is established through the CASPs or crypto-ATMs, which are located in regions or jurisdictions outside the EU and are associated with high levels of predicate offences or the risk of ML/TF.

e) The customer is involved in crypto asset mining operations (either directly or indirectly through relationships with third parties) that take place in a high-risk jurisdiction, identified by the European Commission in accordance with Article 9 of Directive (EU) 2015/849, or in a jurisdiction that is subject to restrictive measures or targeted financial sanctions;

21.8. The factor that may contribute to **reducing risk:**

a) where the transfer comes from or is sent to a crypto asset account or a distributed ledger address that is hosted by a provider of services in crypto assets ecosystem that is regulated and supervised outside the EU under a regulatory framework that is as robust as the one foreseen in Directive (EU) 2015/849 and that foreseen in Regulation (EU) XXXX/XXX[19] and which is associated with low levels of predicate offences.

Distribution channel risk factors

21.9. The following factors may contribute to **increasing risk:**

a) the business relationship is established by using remote customer onboarding solutions that are not compliant with the EBA's Guidelines on Remote Customer Onboarding[20].

b) there are no restrictions on the funding instrument, for example in the case of cash, cheques or electronic money products, that benefit from the exemption under Article 12 of Directive (EU) 2015/849.

[19] Insert reference to MiCA regulation

[20] EBA's Guidelines on the use of Remote Customer Onboarding Solutions under Article 13(1) of Directive (EU) 2015/849 (EBA/GL/2022/15)

c) the business relationship between the CASP and the customer is established through an intermediary service provider in crypto assets ecosystem outside the EU, which is unregulated or is subject to AML/CTF regulatory and supervisory framework that is less robust than the one provided for in Directive (EU) 2015/849.

d) when commencing a business relationship with a customer, the CASP is using services of an outsourcing service provider in accordance with Article 29 of Directive (EU) 2015/849, to gather CDD from the customer, in particular, where that service provider is located in a high-risk jurisdiction.

e) new distribution channels or new technology used to distribute crypto assets that has not been fully tested yet or used before.

f) the business relationship is established via the crypto-ATMs, which increases the risk due to the use of cash.

21.10. The factor that may contribute to **reducing risk**:

a) where the CASP places reliance on CDD measures applied by a third party in accordance with Article 26 of Directive (EU) 2015/849 and where that third party is located in the EU.

Measures

21.11. CASPs should ensure that systems used by them to identify ML/TF risk associated with individual business relationships, transfers or occasional transactions and to identify suspicious transactions comply with the criteria set out in Title I. In particular, CASPs should ensure that they have adequate transaction monitoring and advanced analytics tools in place that are commensurate to the nature and volume of the CASP's activities, including the type of crypto assets made available for trading or exchanged.

Enhanced customer due diligence

21.12. Where the risk associated with a business relationship or occasional transaction is increased, CASPs must apply EDD measures pursuant to Article 18 of Directive (EU) 2015/849 as set out in Title I. In addition, CASPs should apply the following EDD measures:

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 majority shareholders that do not meet the definition of beneficial owners in accordance with Article 3 of Directive (EU) 2015/849 or any natural persons who have authority to operate a crypto asset account or distributed ledger address on behalf of the customer or give instructions concerning the transfer or exchange of crypto assets or other services relating to those crypto assets.

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 CASPs 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 exchanged for crypto assets, to be reasonably satisfied that these are legitimate;
   iii. the source of the customer's crypto assets that are being exchanged for fiat currencies, including when and where they were purchased;
   iv. the purpose of the transaction, including, where appropriate, the destination of the crypto asset transfer;
   v. information on any associations the customer might have with other jurisdictions (headquarters, operating facilities, branches, etc.) and the individuals who may influence its operations;
   vi. to request or obtain data relating to the customer's crypto asset transaction and trading history.

d) obtaining evidence about the source of funds and wealth or the source of crypto assets in respect of all transactions that present a higher risk, including those that involve:
   i. an exchange of crypto assets for cash or vice versa;
   ii. an exchange of one crypto asset for another if the customer claims the crypto asset has been obtained, for example, through mining, airdrops, staking rewards, governance tokens, an Initial Coin Offering (ICO), or crypto lending protocols; or
   iii. the transfer of a customer's crypto assets from one exchange to another or to a self-hosted address.

e) increasing the frequency of monitoring crypto asset transactions. All transactions must be monitored for unexpected behaviours and indicators of suspicious activity and should also include consideration of the parties the customer is transacting with.

f) reviewing and, where necessary, updating information, data and documentation held more frequently and, in particular, in the case of a trigger event.

g) where the risk associated with the relationship is particularly high, CASPs should review the business relationship more regularly.

h) assess more frequently or in more depth the activities performed through the crypto asset accounts used by the customer by using a crypto investigation tool;

i) where a customer has addresses in multiple distributed ledgers or blockchain networks, the CASP should link these addresses to the customer.

j) increasing the frequency of monitoring of the customer's IP addresses and checking them with the IPs used by other customers.

k) obtain confirmation about the customer's level of knowledge and understanding of crypto assets to achieve a level of assurance that the customer is not used as a money mule.

l) where a pattern of withdrawals or redemptions is not in line with the customer's profile or the nature and purpose of the business relationship, the CASP should introduce additional measures to ensure that a withdrawal or redemption is requested by the customer and not by a third party. This is particularly relevant for high risk or elderly or more vulnerable customers.

21.13. CASPs should apply advanced analytics tools to assess the risk of transactions, particularly for transactions involving self-hosted addresses. Based on the nature of the CASP, it might be sufficient to apply advanced analytics tools to transactions on a risk-sensitive basis, as a supplement to the standard transaction monitoring tools. Such tools are crucial to trace the history of transactions, individual coins and to identify links with criminal activities, persons or entities.

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

Simplified customer due diligence

21.15. In low-risk situations, which have been classified as such as a result of the ML/TF risk assessment carried out by the CASP in accordance with these guidelines, and to the

extent permitted by national legislation, CASPs may apply SDD measures, which may include:

a) for customers that are subject to a statutory licensing and regulatory regime in the EU or in a third country, 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) updating CDD information, data or documentation 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, while observing any update periods set out in the national legislation.

c) lowering the frequency of transaction monitoring for products involving recurring transactions, like in the case of portfolio management.

Record keeping

21.16. Where the information on customers and transactions is available on the distributed ledger, firms should not place reliance on the distributed ledger for recordkeeping but should take steps to fulfil their recordkeeping responsibilities in accordance with Directive 2015/849 and Guidelines 5.1 and 5.2 above.

5. Accompanying documents

5.1 Cost-benefit analysis / Impact assessment

As per Article 16(2) of Regulation (EU) No 1093/2010 (EBA Regulation), any guidelines and recommendations developed by the EBA shall be accompanied by an Impact Assessment (IA), which analyses 'the potential related costs and benefits'. This analysis presents the IA of the main policy options included in this Consultation Paper on the *draft Guidelines amending revised Guidelines (EBA/GL/2021/02) 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)* ('the draft Guidelines'). The IA is high level and qualitative in nature.

A. Problem identification and background

Directive (EU) 2015/849, in line with international standards in combating money laundering and the financing of terrorism developed by FATF, puts the risk-based approach at the center of the EU's ML/TF regime. It recognized 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. Articles 17 and 18(4) require the EBA, to issue guidelines, addressed to competent authorities and to the credit institutions and financial institutions, on the risk factors to be taken into consideration and the measures to be taken in situations where simplified customer due diligence measures are appropriate. In this context, the EBA published in 2021 the Guidelines (EBA/GL/2021/02) 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'). These Guidelines were revised in XX 2023 when the EBA amended Guidelines (EBA/GL/2021/02) 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 ('The revised ML/TF Risk Factors Guidelines').

In July 2021, the European Commission published an AML/CFT package consisting of 4 legislative proposals. One of these proposals was the recast of Regulation (EU) 2015/847 ('The Transfer of Funds Regulation' or 'FTR') in order to extend its scope to transfers of crypto assets, in line with the FATF's standards. The co-legislators reached a provisional agreement on the FTR recast on 29th June 2022. In this recast the EBA was given ten legislative mandates and four of them were related to topics that could be addressed in the revised ML/TF Risk Factors Guidelines, as they mandated the EBA to:

a) Determine the application of general EDD to transfers of crypto assets;

b) Define possible EDD measures regarding transfers of crypto assets involving self-hosted wallets;

c) Define the criteria and elements to take into account for deciding EDD measures for correspondent banking relationships with non-EU CASPs; and

d) Identify the risk variables and risk factors to be taken into account by CASPs when entering into business relationships or carrying out transactions in crypto assets.

Furthermore, Article 30(b) of the recast of Regulation (EU) 2015/847 amends Article 3 of Directive (EU) 2015/849 to subject crypto-asset service providers ('CASPs') to the same ML/TF requirements and ML/TF supervision as credit and financial institutions.

To meet the above mandates, the EBA intends to leverage on existing provisions in the revised ML/TF Risk Factors Guidelines.

B. Policy objectives

The objective proposed amendments to the Guidelines is to ensure that *firms identify, assess and effectively manage the ML/TF risk associated with* crypto assets and CASPs.

C. Options considered, assessment of the options and preferred options

Section C. presents the main policy options discussed and the decisions made by the EBA during the development of the draft Guidelines. Advantages and disadvantages, as well as potential costs and benefits from the qualitative perspective of the policy options and the preferred options resulting from this analysis, are provided.

Inclusion of CASPs in the revised ML/TF Risk Factors Guidelines

The revised ML/TF Risk Factors Guidelines are related to credit and financial institutions (altogether 'The firms') and the AML/CFT competent authorities (CAs) supervising those firms. With the Article 30(b) of the recast of Regulation (EU) 2015/847 and the amendment of Article 3 of Directive (EU) 2015/849, CASPs were included in the 'financial institutions' definition and, de facto, included in the revised ML/TF Risk Factors Guidelines. two options have been considered by the EBA in this regard:

Option 1a: Not amending the revised ML/TF Risk Factors Guidelines further than the, de facto, inclusion of the CASPs in the definition of 'financial institutions' foreseen by the modification of Article 3 of Directive (EU) 2015/849.

Option 1b: Amending the revised ML/TF Risk Factors Guidelines further than the, de facto, inclusion of the CASPs in the definition of 'financial institutions' foreseen by the modification of Article 3 of Directive (EU) 2015/849.

The EBA performed a review of the revised ML/TF Risk Factors Guidelines and concluded that the elements set out in these guidelines could be extended to CASPs but also that CASPs had specific characteristics differentiating them from credit institutions and other financial institutions and thus these specificities together with crypto-assets' inherent ones would benefit from further guidance and clarification. For instance, as CASPs products and services offered differ from credit institutions and other financial institutions' products and services, adding guidance, specifically addressed to CASPs, on the risk factors related to these products and services could be of benefit for CASPs. An example is the product's increasing-risk factor when CASPs products entail privacy-enhancing features or offer a higher degree of pseudonymity such as mixers or tumblers, obfuscated ledger technology, Internet Protocol (IP) anonymizers, ring signatures, stealth addresses, ring confidential transactions, atomic swaps, non-interactive zero-knowledge proofs and so-called privacy coins. Another example is that as the area of crypto assets is new, different of other assets' areas and in constant evolution, additional guidance on firms' staff's AML/CFT trainings regarding crypto assets unusual transactions or more advanced transaction monitoring analytical tools would be of benefit.

For firms, and more particularly CASPs, the costs related to the amendments of the revised ML/TF Risk Factors Guidelines are not deemed to be material as compliance with these guidelines is necessary to ensure compliance with the underlying legal obligations in Directive (EU) 2015/849. For competent authorities, the costs will arise mainly from reviewing amended regulatory guidance of firms (mostly for CASPs) and supervisory manuals to ensure consistency with these guidelines. The benefits of the amendments for competent authorities are that the guidelines will help supervisors to communicate and set clear expectations of the factors CASPs should consider when identifying and assessing ML/TF risk and deciding on the appropriate level of CDD.

On these grounds, **the Option 1b has been chosen as the preferred option** and the draft Guidelines will amend the revised ML/TF Risk Factors Guidelines further than the, de facto, inclusion of the CASPs in the definition of 'financial institutions' foreseen by the modification of Article 3 of Directive (EU) 2015/849.

D. Conclusion

The development of draft Guidelines amending revised Guidelines (EBA/GL/2021/02) 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 revised ML/TF Risk Factors Guidelines') under Articles 17 and 18(4) of Directive (EU) 2015/849) was deemed necessary to take into account the crypto-assets and the CASPs and the impact this has on AML/CFT risk factors. The costs associated with the amendments of the draft Guidelines will be exceeded by the aforementioned benefits. These draft Guidelines hence should achieve, with acceptable costs, their objectives of ensuring that the ML/TF Risk

Factors Guidelines will meet the mandates and take into account the crypto assets and related development of CASPs.

5.2 Overview of questions for consultation

Question 1: Do you have any comments on the proposed changes to definitions.

Question 2: Do you have any comments on the proposed changes to Guideline 1.

Question 3: Do you have any comments on the proposed changes to Guideline 2.

Question 4: Do you have any comments on the proposed changes to Guideline 4.

Question 5: Do you have any comments on the proposed changes to Guideline 6.

Question 6: Do you have any comments on the proposed changes to Guideline 8.

Question 7: Do you have any comments on the proposed changes to Guideline 9.

Question 8: Do you have any comments on the proposed changes to Guideline 10, 15 and 17.

Question 9: Do you have any comments on the proposed changes to Guideline 21.