EBA/GL/2024/01

16 January 2024

Final Report

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. Executive Summary

These Guidelines amend the EBA's revised ML/TF Risk-Factors Guidelines (EBA/GL/2021/02). They foster a common understanding of ML/TF risks associated with crypto-assets service providers (CASPs) and the steps CASPs and other credit and financial institutions should take to manage these risks.

The amending Guidelines:

- Insert risk factors in Title I of the Guidelines that are specific to crypto-assets and CASPs.
- Provide guidance in Title II for credit and financial institutions on the ML/TF risks associated with customers that are providing crypto-assets services, but which are not authorised or regulated in accordance with Regulation (EU) 2023/1114 on markets in crypto-assets, and amending Regulations (EU) No 1093/2010 and (EU) No 1095/2010 and Directives 2013/36/EU and (EU) 2019/1937.
- Provide sector-specific guidance for CASPs in Title II of the ML/TF Risk Factors Guidelines (Guideline 21) on the factors that CASPs should consider when assessing ML/TF risks associated with their business relationships. In addition to ML/TF risk factors set out in Title I of the Guidelines, CASPs should also consider risks associated with:
    - transactions, such as transfers to or from self-hosted addresses, decentralised platforms or transfers involving providers of crypto-assets services that are not authorised or regulated in accordance with Regulation (EU) 2023/1114;
    - products, such as those containing anonymity-enhancing features or which allow transfers to and from the CASP and self-hosted and decentralised trading platforms;
    - the nature of customers and their behaviour, including when customers provide inconsistent or incorrect information or their transaction volumes or patterns are not in line with those expected from the type of customer;
    - the customers' or beneficial owners' links to high-risk jurisdictions or transactions to/from jurisdictions associated with a high risk of ML/TF.
- In Title II, provide guidance on mitigating measures CASPs should apply:

- in situations where the ML/TF risk is increased, including the circumstances which may warrant the use of advanced analytics tools as part of monitoring of business relationships;

- in lower ML/TF risk situations, to the extent that this is permitted by national law.

Next steps

The Guidelines will be translated into the official EU languages and published on the EBA's website. The deadline for competent authorities to report whether they comply with the Guidelines will be 2 months after the publication of the translations. The Guidelines will apply from 30 December 2024.

2. 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. Regulation (EU) 2023/1113 on information accompanying transfers of funds and certain crypto-assets and amending Directive (EU) 2015/849 (recast) (the 'Regulation') was part of the proposals. It was published on 9 June 2023.

2. The Regulation amends the scope of Directive (EU) 2015/849 by subjecting CASPs, which have been authorised under Regulation (EU) 2023/1114, to the same AML/CFT requirements and AML/CFT supervision as other credit institutions and financial institutions.

3. Article 38 of Regulation (EU) 2023/1113 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, including transactions originating from or directed to self-hosted addresses. It also introduced new provisions in Article 19b to Directive (EU) 2015/849, mandating the EBA to clarify the due diligence requirements CASPs should apply in high ML/TF risk situations, and when entering into correspondent relationships with respondents that are CASPs from non-EU countries.

4. To fulfil this mandate, the EBA decided to amend the EBA's Guidelines (EBA/2021/02) on customer due diligence (CDD) 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').

5. The EBA publicly consulted on a draft version of these amending Guidelines between 31 May and 31 August 2023. A public hearing took place on 7 June 2023. Twenty-one respondents provided comments, which the EBA considered when preparing the final version of these Guidelines.

6. These Guidelines amend the revised Risk Factors Guidelines. A consolidated version will be published on the EBA's website.

3.2. Rationale

7. Upon receipt of its mandate under Regulation 2023/1113, the EBA performed an analysis of existing instruments to determine whether new or amended guidelines were necessary to fulfil this mandate.

8. 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 suitable CDD measures set out in Title I of the Risk Factors Guidelines should apply to CASPs as it does to other 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.

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

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

Amendments to Subject matter, scope and definitions

11. The amended Guidelines clarify that the definitions set out in Directive (EU) 2015/849 and Regulation (EU) 2023/1113 also apply to these Guidelines.

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

12. The Guideline sets out general principles that credit and financial institutions (firms), need to apply when assessing ML/TF risks associated with their business and individual business relationships. These principles apply to CASPs as they do to other firms. 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 or making significant changes to the existing practices, products or services.

Amendments to Guideline 2: Identifying ML/TF risk factors

13. 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. Amendments to Guideline 2.4 provide that firms should consider whether their customers' business activities involving crypto-assets may expose these firms to an increased ML/TF risk.

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

14. This Guideline explains what firms should consider 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 business models is based on remote customer onboarding, the proposed amendments highlight the need for CASPs and other firms to ensure compliance with the EBA's Guidelines (EBA/GL/2022/15) on the use of remote customer onboarding solutions.

15. 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 amendments recognise that transactions that are more frequent than usual or transactions involving small amounts that are unusually frequent or transactions without an obvious economic rationale may be indicators of unusual transactions. In addition, proposed amendments to Guideline 4.74 emphasise the need for suitable transaction monitoring systems to be put in place by firms and specify that, in some circumstances, advanced analytics tools might be warranted for CASPs due to the level of ML/TF risks.

Amendments to Guideline 6: Training

16. Guideline 6 specifies that firms should provide suitable 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.

Amendments to Guideline 8: Sectoral Guideline for correspondent relationships

17. In this Guideline, the EBA provides guidance to firms when they engage in a correspondent relationship with a respondent. 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 when they engage in a correspondent relationship defined in Article 3(8) of Directive (EU) 2015/849.

18. Amended Guideline 8 specifies the firms' obligations 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, other than CASPs authorised under Regulation (EU) 2023/1114, or where they are deemed to present an increased ML/TF risk as explained in Guideline 21.3(d).

Amendments to Guideline 9: Sectoral Guideline for retail banks

19. Amendments to these Guidelines recognise that, as a result of changes in the legislative framework introduced by Regulation (EU) 2023/1114, CASPs will be engaging increasingly with or be customers of credit institutions. The Guidelines now specify that banks may be exposed to increased risks where they engage in business relationships with those providers of crypto-asset services which are not regulated and supervised under Regulation (EU) 2023/1114.

Amendments to Guideline 10, Guideline 15 and Guideline 17

20. These are guidelines addressed to firms in different sectors. Amendments clarify that firms should also consider Guideline 21, where they engage in a similar business to that of CASPs or have business relationships with CASPs.

21. In Guideline 17, the term 'virtual currencies' was replaced with 'crypto-assets' as defined in Regulation (EU) 2023/1113.

Guideline 21: Sectoral Guideline for crypto-asset service providers (CASPs)

22. 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 Guideline clarifies regulatory expectations for CASPs when they identify and assess ML/TF risks associated with their overall business and with individual business relationships.

23. In particular, the Guideline acknowledges that CASPs' products, which are designed in a way that allows transfers to and from e.g. self-hosted addresses and any type of decentralised trading platforms or protocols may expose them to an increased ML/TF risk due to the lack of regulatory framework and the absence of the identification and verification requirements applicable to their users. The Guideline also recognises that an increased risk may be presented by some of the CASPs' product features which facilitate anonymity such as, but not limited to, mixers or tumblers, obfuscated ledger technology, ring signatures, stealth addresses, ring confidential transactions, atomic swaps and non-interactive zero-knowledge proofs. Equally, transfers to and from platforms that obfuscate transactions and foster anonymity, expose CASPs to increased risks. 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 ML/TF risk.

24. Furthermore, Guideline 21 provides a non-exhaustive list of enhanced and simplified CDD measures that CASPs should consider applying to their business relationships which are exposed to increased or low risk of ML/TF. The extent of these measures should be determined by CASPs and set out in their policies and procedures. 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 particular case for the monitoring of customers and their transactions, where the guidelines require that CASPs have appropriate procedures and systems in place to monitor all types of transactions and crypto-assets. CASPs should also determine circumstances when the use of advanced analytics tools is warranted in their business.

Editorial amendments

25. Finally, the EBA made a number of changes that are of an editorial, presentational or structural nature.

3. Guidelines amending Guidelines EBA/2021/02

EBA/GL/2024/01

16 January 2024

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

2. Guidelines set the EBA's view of appropriate supervisory practices within the European System of Financial Supervision or of how EU 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/2024/01'. Notifications should be submitted by persons with appropriate authority to report on compliance on behalf of their competent authorities. Any change in the status of compliance must also be reported to the EBA.

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

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

2. Subject matter, scope and definitions

Addressees

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

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

3. Implementation

Date of application

6. These Guidelines apply from 30 December 2024.

4. Amendments

(i) Amendment to the title of the Guidelines

7. The title of the Guidelines is replaced by the following:

'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 Directive (EU) 2015/849'

(ii) Amendments to subject matter, scope and definitions

8. In paragraph 12, the introductory phrase is replaced by the following:
'Unless otherwise specified, terms used and defined in Directive (EU) 2015/849 and Regulation (EU) 2023/1113 have the same meaning in the Guidelines. In addition, for the purposes of these Guidelines, the following definitions apply:'

9. In paragraph 12, point (f) and point (m) are deleted.

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

10. In Guideline 1.7, the following point is added:

'd) Where the firm is launching new products, services, or business practices, or significantly changing them, including where it introduces a new delivery channel, or adopts 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 of these products, services or business practices. Where these products, services or business practices have a significant impact on the firm's ML/TF risk exposure, the firm should reflect this assessment in its business-wide risk assessment carried out in accordance with Article 8(2) of Directive (EU) 2015/849 and its policies and procedures.'

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

11. In Guideline 2.4, point b) is replaced by the following:

'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, providers of crypto-assets services as described in Guidelines 9.20 and 9.21, casinos or dealers in precious metals?'

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

12. In Guideline 4.29, the introductory phrase is replaced by the following:

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

13. Guideline 4.35 is replaced by the following:

'4.35 Where the external provider is a firm established in a non-EU 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, including in case of termination of an outsourcing agreement.'

14. In Guideline 4.60, point a) is replaced by the following:

'a) they differ from the transactions the firm would normally expect based on its knowledge of the customer the business relationship or the category to which the customer belongs, either in the amount or frequency or complexity or similar, including when transactions are larger or more frequent than usual or for transactions involving small amounts that are unusually frequent, or where there are successive transactions without an obvious economic rationale, such as transactions that are split up to circumvent reporting limits or align unusual transactions with the normally expected behaviour and patterns as supported by information gathered during the on-boarding procedure and the ongoing monitoring of the business relationship.'

15. In Guideline 4.61, point a) is replaced by the following:

'a) taking reasonable and appropriate measures to understand the background and purpose of these transactions, for example by determining 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'

16. In Guideline 4.74, point b) is replaced by the following:

'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;'

17. In Guideline 4.74, the following point is added:

'd) whether the use of advanced analytics tools, like distributed ledger or blockchain 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.'

(vi) Amendments to Guideline 6: Training

18. In Guideline 6.2, point c) is replaced by the following:

'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;'

19. In Guideline 6.2, the following point is added:

'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.'

(vii) Amendments to Guideline 8: Sectoral Guideline for correspondent relationships

20. In Guideline 8.6, point d) is replaced by the following:

'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 crypto-assets services, other than CASPs regulated under Regulation (EU) 2023/1114[3], which are bound by an AML/CFT regulatory and supervisory regime that is less robust than the regime envisaged in Directive (EU) 2015/849 or are not subject to any AML/CFT obligations;
iv. significant business on behalf of CASPs, for which the business model is focused on providing products and services described in Guideline 21.3(d);
v. business with non-residents; or
vi. business in a currency other than that of the country in which it is based.'

21. In Guideline 8.6, the following point is added:

[3] Regulation (EU) 2023/1114 on markets in crypto-assets, and amending Regulations (EU) No 1093/2010 and (EU) No 1095/2010 and Directives 2013/36/EU and (EU) 2019/1937

'h) the IBAN account provided by a respondent CASP where it receives funds in an official currency[4] from customers is in the name and ownership of a company, which is not the respondent CASP's company or in any way known to be linked to the respondent CASP.'

22. In Guideline 8.8, the following point is added:

'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 through the verification of the internet protocol (IP) addresses of its customers or other means, in circumstances where it is required by the respondent's policies and procedures.'

23. In Guideline 8.17, point a) and point c) are replaced by the following:

'a) Gather sufficient information about a respondent institution to understand fully the nature of the respondent's business, to determine 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 the 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.'

(viii) Amendments to Guideline 9: Sectoral Guideline for retail banks

24. Guideline 9.3 is replaced by the following:

'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 sectoral Guideline 18 and those that provide crypto-asset services should refer to

[4] Article 3, point (8) of Regulation (EU) 2023/1114 defines official currency as an official currency of a country that is issued by a central bank or other monetary authority.

sectoral Guideline 21.'

25. Guideline 9.16 is replaced by the following:

'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.'

26. Guideline 9.17 is replaced by the following:

'9.17 Where a bank has determined, based on its ML/TF risk assessment carried out in keeping 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.'

27. In Guideline 9.18, the introductory phrase is replaced by the following:

'9.18. However, to the extent permitted by national legislation, where, according to the individual ML/TF risk assessment of the customer, the risk associated with the business relationship is low, a bank may apply simplified due diligence (SDD) measures, provided that:'

28. The heading of Guidelines 9.20 to 9.24 is replaced by the following:

'Customers that offer services related to crypto-assets'

29. Guidelines 9.20 to 9.23 are deleted.

30. The following Guidelines 9.20 and 9.21 are inserted:

'9.20 When entering into a business relationship with a customer who is a provider of crypto-assets services, other than a CASP regulated under Regulation (EU) 2023/1114[5], banks may be exposed to increased risk of ML/TF. The risk may be reduced in circumstances where such a provider is regulated and supervised under a regulatory framework similar to that set out in Regulation (EU) 2023/1114 or Directive (EU) 2015/849. Banks should carry out the ML/TF risk assessment of these customers prior to establishing a business relationship with them. As part of this, banks should also consider the ML/TF risk associated with the specific type of crypto-assets that are provided or serviced by these providers.'

'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:

[5] Regulation (EU) 2023/1114 on markets in crypto-assets, and amending Regulations (EU) No 1093/2010 and (EU) No 1095/2010 and Directives 2013/36/EU and (EU) 2019/1937.

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 CDD measures to their clients either under a legal obligation or on a voluntary basis;

d) determine whether the customer is registered or licensed in an EU/EEA Member State or a non-EU country, and, in the case of a non-EU country, take a view on the adequacy of that non-EU country's AML/CFT regulatory and supervisory regime in accordance with Guideline 2.11;

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

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

g) where the customer's business involves issuing crypto-assets to raise funds, such as Initial Coin Offerings, banks should determine whether such business is performed in compliance with existing legal requirements and, where applicable, whether it is regulated for AML/CFT purposes according to internationally agreed standards, such as standards published by the Financial Action Task Force.'

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

31. Guideline 10.2 is replaced by the following:

'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.'

(x) Amendments to Guideline 15: Sectoral Guideline for investment firms

32. Guideline 15.1 is replaced by the following:

'15.1. Investment firms as defined in Article 4(1)(1) of Directive 2014/65/EU should consider when providing or executing investment services or activities as defined in Article 4(1)(2) of Directive (EU) 2014/65 the following risk factors and measures alongside those set out in Title I of these Guidelines. Sectoral Guideline 12 and Guideline 21 may also be relevant in this context.'

(xi) Amendments to Guideline 17 Sectoral Guideline for regulated crowdfunding platforms

33. In Guideline 17.4, point i) is replaced by the following:

' i). The CSP allows the use of crypto-assets by investors and project owners to settle their payment transactions through the crowdfunding platform, where such transfers may be exposed to an increased risk of ML/TF due to factors described in Guideline 21.3(d).'

34. In Guideline 17.6, point b) is replaced by the following:

'b) The investor or the project owner transfer crypto-assets, where such a transfer may be exposed to an increased risk of ML/TF due to factors described in Guideline 21.3, point (d).'

35. The following Guideline 21 is inserted:

(xii) '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 the 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 that offer a higher degree of anonymity.

21.2. When offering crypto-asset services, CASPs should comply with provisions in Title I as well as sector-specific provisions set out in Title II where these are relevant to the CASP's product offering.

Risk factors

Product, services and transaction risk factors

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

a) the products or services provided by a CASP offer a higher degree of anonymity;

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

c) the product places no upfront 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 crypto-assets services as defined in Guideline 9.20 or which is subject to the AML/CFT regulatory and supervisory regime that is less robust than the regime envisaged in Directive (EU) 2015/849;
   iii. a peer-to-peer cryptocurrency exchange platform or another type of decentralised or distributed crypto-assets application, which is not controlled or influenced by a legal or natural person (often referred to as 'decentralised finance' (DeFi));
   iv. platforms that aim to obfuscate transactions and facilitate anonymity such as mixer or tumbler platforms;
   v. hardware used to exchange crypto-assets to official currencies or vice versa (such as crypto-ATMs), 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 channels, and the use of technologies where the level of the ML/TF risk cannot be reliably assessed by the CASP in accordance with Guideline 1.7, point (d) due to the lack of information;

f) where the wholesale CASP exercises a weak control over the nested service provided by another CASP;

g) the results of an analysis ran by advanced analytics tools indicate an increased level of risk.

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 allows transactions between the customer's account and

   i. crypto-asset accounts or distributed ledger addresses in the customer's name held by a CASP;
   ii. a crypto-asset account or distributed ledger address in the customer's name, that is held by a provider of crypto-assets services, other than a CASP regulated under Regulation (EU) 2023/1114[6], which is regulated outside the EU under the regulatory framework, that is as robust as that envisaged in Regulation (EU) 2023/1114and which is subject to AML/CTF regulatory and supervisory framework that is as robust as the one provided for in Directive (EU) 2015/849;
   iii. a bank account in the customer's name at a credit institution that is 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; or

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 a limited and defined group 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 the 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, which is a shell bank, as defined in Article 3(17) of Directive (EU) 2015/849, or another type of shell company;
   iii. a company, that has been recently established and is processing large volumes of transactions;
   iv. a legally registered company that is processing large volumes of

[6] Regulation (EU) 2023/1114 on markets in crypto-assets, and amending Regulations (EU) No 1093/2010 and (EU) No 1095/2010 and Directives 2013/36/EU and (EU) 2019/1937

transactions after a period of inactivity since it was established;

v. an undertaking, which is in a business relationship with another undertaking(s) within the group as defined in Article 3(15) of Directive (EU) 2015/849 that provides products and services related to crypto-assets;

vi. an undertaking or a person who is using an IP address associated with a darknet or a software that allows anonymous communication, including encrypted emails, anonymous or temporary email services and VPNs;

vii. a vulnerable person, meaning a person who is not likely to be a typical customer of a CASP, or a person who displays very little knowledge and understanding of crypto-assets or the related technology, which may be evidenced by the results of an appropriateness/knowledge test or through other engagements with the customer, and who nevertheless chooses to make frequent or high-value transactions, 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 with no apparent economic rationale or business purpose.

ii. or the customer's beneficial owner is unable or unwilling to provide the necessary CDD information, when requested by the CASP, without any legitimate reason for it, by:
   a) deliberately avoiding direct contact with a CASP, either in person or remotely;
   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 obtain 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 necessary to accompany a transfer in accordance with Article 14(1) and 14(2) of Regulation (EU) 2023/1113, or the customer's habitual 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. Is using an address, a location or an IP address linked to crypto-asset accounts registered to different users held with a single CASP or with multiple CASPs.

vi. Frequently changes its personal information or its payment instruments without obvious reason.

vii. Frequently receiving or transferring such amounts of crypto-assets from self-hosted addresses, which are just below the EUR 1 000 threshold defined in Article 14(5) and Article 16(2) of Regulation (EU) 2023/1113 triggering the verification of the beneficiary or the originator.

viii. Indicates that the purpose is to invest in an initial public offering of tokens or in a crypto-asset or product that offers a disproportionately high return and is based in a high-risk jurisdiction or is associated with high fraud-related indications or which is not supported by a white paper required under the Regulation (EU) 2023/1114[7].

ix. Displays behaviour or transaction patterns which are 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 has 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 and volume 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 to an extent that is not commensurate with the customer's declared income or it otherwise exceeds the expected volume of activity.

x. Displays behaviour and patterns, which are unusual because they involve unexplained transfers to/from distributed ledger addresses or

[7] Regulation (EU) 2023/1114 on markets in crypto-assets, and amending Regulations (EU) No 1093/2010 and (EU) No 1095/2010 and Directives 2013/36/EU and (EU) 2019/1937.

crypto-assets accounts in multiple jurisdictions with no apparent business or lawful purpose.

xi. When exchanging crypto-assets to official 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 providers of payment services;
   e) repeatedly requests an exchange of crypto-assets to or from cash or anonymous electronic money;
   f) uses protocols that connect two blockchains, to exchange crypto-assets to other crypto-assets on a different network, such as Monero, Zcash or similar;
   g) uses Crypto-ATMs in different locations to repeatedly transfer funds to a bank account;
   h) withdraws crypto-assets from a CASP to a self-hosted address immediately after depositing crypto-assets or exchanging for different crypto-assets in a CASP.

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) 2023/1114 or under any other relevant regulatory framework within or outside the EU and, which is notably a decentralised or distributed application with no legal or natural person with control or influence over it.

xiii. Directly or indirectly receives or sends crypto-assets that are associated with the darknet or that are the result of illegal activities.

xiv. Is investing or exchanging crypto-assets, which themselves offer a higher degree of anonymity or the customer receives crypto-assets which have been subject to anonymity-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 crypto-asset service provider, which does not fall within the scope of Regulation (EU) 2023/1114 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 crypto-asset accounts held by the same or different CASPs without an apparent economic rationale for it;

c) a newly created or previously inactive 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 or a transfer from such an account in a short period of time without an apparent economic rationale for it;

f) a crypto-asset account frequently below a defined threshold or, in case of transfers to a self-hosted address, below the threshold of EUR 1 000 as defined in Article 14(5) and Article 16(2) of the Regulation (EU) 2023/1113;

g) a crypto-asset account by splitting the transactions into multiple transactions which are sent to multiple distributed ledger addresses by using smurfing techniques.

xvi. The customer appears to exploit technological glitches or failures to their advantage.

xvii. The customer explains that the crypto-assets transferred to the CASP have been obtained through mining or staking rewards, but these rewards do not appear to be proportionate to the crypto-assets generated through such activities.

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

a) the customer has complied with the information requirements provided for in Regulation (EU) 2023/1113 and as further specified in Section 4 of the EBA's Travel Rule Guidelines[8], during previous transactions in crypto-assets and has provided information that enables the identification of a customer or the ability to check it if there is doubt or suspicion;

[8] Guidelines on preventing the abuse of funds and certain crypto-assets transfers for money laundering and terrorist financing purposes under Regulation (EU) 2023/1113, […. please insert here the number of these GL once adopted', at present under consultation (EBA/CP/2023/35)] ('The Travel Rule Guidelines')

b) 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) the customer requests an exchange to/from official currency and either the source 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) the customer requests an exchange and either the source or destination of the crypto-asset is the customer's own crypto-asset account or a distributed ledger address, which is hosted either by a CASP regulated under Regulation (EU) 2023/1114 or by a provider of crypto-assets services, other than a CASP, which is regulated and supervised outside the EU under the regulatory framework that is as robust as that envisaged in Regulation (EU) 2023/1114 and, which is subject to AML/CFT requirements as robust as those envisaged in Directive (EU) 2015/849, that has been whitelisted or otherwise determined by the CASP as low risk;

e) the customer requests an exchange and either the source or destination of the crypto-asset relates to low value payments for goods and services to/from a crypto-asset account or a distributed ledger address on which there is no adverse information available;

f) the customer transfers between two CASPs or a CASP and a crypto-asset service provider, other than a CASP, which is either subject to regulation and supervision within the EU or is otherwise subject to a regulatory framework that is as robust as that envisaged in Regulation (EU) 2023/1114 and, which is subject to AML/CFT requirements as robust as those envisaged in Directive (EU) 2015/849.

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 relationships involving 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 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 personal or business relationships involving a jurisdiction associated with an increased ML or TF risk.

d) The business relationship is established through a CASP or a crypto-ATM, which is located in a region or a jurisdiction that is associated with high levels of the ML/TF risk.

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 CASP or a crypto-assets services provider other than a CASP, in a jurisdiction associated with low levels of the ML/TF risk.

Distribution channel risk factors

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

a) The business relationship is established by using remote customer on-boarding solutions that are not compliant with the EBA's Guidelines on Remote Customer Onboarding[9].

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.

c) The business relationship between the CASP and the customer is established through an intermediary crypto-assets service provider defined in Guideline 9.20 above.

d) The identification and verification of a customer is carried out by a crypto-assets service provider located in a high-risk jurisdiction on the basis of an

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

outsourcing agreement, in accordance with Article 29 of Directive (EU) 2015/849.

e) New distribution channels or new technology used to distribute crypto-assets, that have not yet been fully tested or that present an increased level of ML/TF risk.

f) The business relationship is established via crypto-ATMs, which increases 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 the systems they use to identify and tackle ML/TF risks comply with the criteria set out in Title I of these Guidelines. In particular, due to their business models, CASPs should ensure that they have suitable and effective monitoring tools in place, including transaction monitoring tools and advanced analytics tools. The extent of such tools is determined by the nature and volume of the CASP's activities, including the type of crypto-assets made available for trading or exchange. CASPs should also ensure that relevant employees receive specialised training to have a good understanding of crypto-assets and ML/TF risks to which they may expose the CASP.

Enhanced customer due diligence

21.12. Where the risk associated with a business relationship or occasional transaction is increased, CASPs have to apply enhanced CDD measures pursuant to Article 18 of Directive (EU) 2015/849 and as set out in Title I of these Guidelines. In addition, CASPs should apply relevant enhanced CDD measures enumerated in the list below, as necessary, depending on the risk exposure of the business relationship:

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

b) Identify and verify 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 on the transfer or exchange of crypto-assets or other services relating to those crypto-assets.

c) Obtain 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 official 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.) or individuals who are known to exercise a significant influence on the customer's operations;

   vi. to request or obtain data about the customer's crypto-asset transactions and, where the customer is a CASP, its trading history from within the CASP's system.

d) Obtain evidence about the source of funds, the source of wealth or the source of crypto-assets in respect of those transactions that present a higher risk.

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

f) Review and, where necessary, update 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 customer's crypto-asset accounts by using crypto-assets investigation tools.

i) Where a customer has multiple distributed ledger addresses or blockchain networks, the CASP should link these addresses to the customer.

j) Increase the frequency of monitoring of the customer's IP addresses and checking them against the IP addresses 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 add 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.

m) Obtain confirmation that a self-hosted address, from which a transfer is received, is under the control or ownership of the CASP's customer.

21.13. CASPs should apply advanced analytics tools to transactions on a risk-sensitive basis, as a supplement to the standard transaction monitoring tools. CASPs should apply advanced analytics tools to assess the risk associated with transactions, particularly transactions involving self-hosted addresses, as it allows the CASP to trace the history of transactions and to identify potential links with criminal activities, persons or entities.

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

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 keeping with these Guidelines, and to the extent permitted by national legislation, CASPs may apply SDD measures, which may include:

a) for customers subject to a statutory licensing and regulatory regime in the EU or in a non-EU 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 if there are 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.

Record keeping

21.16. Where the information on customers and transactions is available on the distributed ledger, CASPs should not place reliance on the distributed ledger for recordkeeping but should take steps to fulfil their recordkeeping responsibilities in accordance with Directive (EU) 2015/849 and Guidelines 5.1 and 5.2 above. CASPs should put in place procedures that allow them to associate the distributed ledger address to a private key controlled by a natural or legal person.

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 Financial Action Task Force (FATF), puts the risk-based approach at the centre of the EU's ML/TF regime. It recognised that the risk of ML/TF can vary and that Member States, CAs 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 CAs and to credit institutions and financial institutions, on the risk factors to consider and the measures to be taken in situations where simplified CDD measures are appropriate. In this context, in 2021, the EBA published the Guidelines (EBA/GL/2021/02) on CDD 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 amended in March 2023 by the EBA's Guidelines (EBA/GL/2023/03) on CDD 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 four legislative proposals. One of these proposals was the recast 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 29 June 2022. Thereafter, Regulation (EU) 2023/1113[10] (the 'Regulation') was published in the Official Journal on 9 June 2023, which gave the EBA a total of 10 legislative mandates. Four of those mandates relate

[10] Regulation (EU) 2023/1113 of the European Parliament and of the Council of 31 May 2023 on information accompanying transfers of funds and certain crypto-assets and amending Directive (EU) 2015/849 (recast).

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) determine possible EDD measures regarding transfers of crypto-assets involving self-hosted addresses;

c) determine the criteria and factors to consider 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 38(2) of the Regulation amends Article 3 of Directive (EU) 2015/849 to define CASPs as obliged entities, which means that the same AML/CFT requirements will apply to them as those applicable to credit and financial institutions. According to the new legal framework, the AML/CFT supervision of CASPs should be done on a risk-sensitive basis.

To meet the above mandates, the EBA intends to leverage 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 CAs supervising those firms. With Article 38(2) of the Regulation 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' envisaged by the amendment 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' envisaged by the amendment 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 items set out in these Guidelines could be extended to CASPs, but also that CASPs present some specific risks that should be considered by credit institutions and financial institutions when entering into a business relationship with them. Therefore, they would benefit from further guidance and clarification on these risks. For instance, products and services offered by CASPs differ from those provided by credit institutions and financial institutions. Adding guidance specifically addressed to CASPs on the risk factors related to these products and services could help CASPs to identify and address these risks before they have crystallised. In particular, where CASPs products entail anonymity-enhancing features or offer a higher degree of pseudonymity such as mixers or tumblers, obfuscated ledger technology, ring signatures, stealth addresses, ring confidential transactions, atomic swaps and non-interactive zero-knowledge proofs. Furthermore, as the CASPs sector is new to AML/CFT requirements, with some CASPs having never been regulated or supervised for AML/CFT purposes, additional guidance on different checks that should be implemented by them to mitigate different levels of risk, such as suitable training, enhanced CDD and the use of blockchain analytics 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 under Directive (EU) 2015/849. For CAs, the costs will arise mainly from reviewing amended regulatory guidance of firms, mostly for CASPs, and supervisory manuals to ensure their compliance with these Guidelines. The benefits of the amendments for CAs 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, **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' envisaged by the amendment of Article 3 of Directive (EU) 2015/849.

D. Conclusion

The development of draft Guidelines amending revised Guidelines (EBA/GL/2021/02) on CDD 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 ML/TF risk factors presented by crypto-assets and CASPs and to explain the factors to be considered by CASPs when entering into business relationships with their customers. Overall, the Guidelines will harmonise the way risk associated with CASPs is assessed by credit and financial institutions across the EU, which may also reduce the de-risking of this sector. 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 Feedback on the public consultation

The EBA publicly consulted on the draft Guidelines contained in the Consultation Paper amending the revised Risk Factors Guidelines. The consultation period lasted for 3 months and ended on 31 August 2023. Twenty-one responses were received, of which 18 were published on the EBA's website. This section presents a summary of the key points arising from the consultation responses. The feedback table in the following section provides further details on other comments received, the analysis performed by the EBA triggered by these comments and the actions taken to address them, where action was deemed necessary. In those instances where several respondents made similar comments or the same respondent repeated comments in the response to different questions, the comments and the EBA analysis are included where the EBA considers them most appropriate. Changes to the draft Guidelines have been incorporated as a result of the responses received during the public consultation.

Summary of key issues and the EBA's response

The EBA asked respondents to reply to the following nine questions:

1. Do you have any comments on the proposed changes to definitions?
2. Do you have any comments on the proposed changes to Guideline 1?
3. Do you have any comments on the proposed changes to Guideline 2?
4. Do you have any comments on the proposed changes to Guideline 4?
5. Do you have any comments on the proposed changes to Guideline 6?
6. Do you have any comments on the proposed changes to Guideline 8?
7. Do you have any comments on the proposed changes to Guideline 9?
8. Do you have any comments on the proposed changes to Guideline 10, 15 and 17?
9. Do you have any comments on the proposed changes to Guideline 21?

Respondents broadly welcomed and supported the changes to the Guidelines proposed by the EBA and viewed them as a positive step towards harmonising the approach and standards applied to and by CASPs. In particular, the respondents welcomed the common understanding, set out in the Guidelines, of the risk-based approach that credit and financial institutions will need to apply when engaging with CASPs, as this may reduce the de-risking of this sector.

Some respondents considered that obligations applicable to CASPs were too detailed compared to the obligations applicable in other sectors. They said that this may put a disproportionate burden on the CASPs sector and may disrupt its growth. The EBA refers to the Opinion (EBA/Op/2023/08) on ML/TF risks affecting the EU's financial sector, which highlights that crypto-assets continue to be exposed to significant ML/TF risks. The Opinion explains that while crypto-assets have existed for roughly a decade, they have remained largely unregulated and unsupervised. Thus, providers of crypto-assets services are less mature in terms of their compliance efforts than other obliged entities under Directive (EU) 2015/849. Therefore, Guidelines are drafted in such a way that they provide a non-exhaustive list of potential risk factors and measures that should help CASPs with their risk assessments, particularly where they have not been obliged entities before this.

Several respondents argued that transactions with self-hosted addresses or decentralised trading platforms do not present an increased ML/TF risk as suggested in the Guidelines. They highlighted various advantages offered by self-hosted addresses to their users like the direct control and increased security as the ability to engage with many parts of the blockchain ecosystem like decentralised finance applications. In respondents' views, the approach to self-hosted addresses in the Guidelines should be more nuanced by recognising that some self-hosted addresses, which have been identified through advanced analytics and other monitoring tools as being linked to suspicious transactions, may present a higher risk than others. The EBA is of the view that transactions with self-hosted addresses and decentralised trading platforms present an increased risk due to the lack of a legal framework applicable to them and the lack of identification and verification requirements applicable to their users. Therefore, the relevant provisions in the Guidelines remain unchanged.

5.3 Summary of responses to the consultation and the EBA's analysis

General feedback on the Guidelines			
Guideline	**Summary of responses received**	**EBA analysis**	**Amendments to the proposal**
Feedback on responses to Question 1: Comments on definitions?			
Definitions	One respondent suggested refraining from using the words CASPs and firms separately, as 'firm' should automatically apply to CASP as well, unless, when for example, CASP is excluded.	The amending Guidelines have been aligned with the structure in the existing EBA's Guidelines on Risk Factors where the term 'firm' is used in Title I (General Guidance) and references to specific financial institutions (i.e. banks, money remitters, e-money issuers, CASPs, etc.) in Title II (the Sector-Specific Guidance).	None
Feedback on responses to Question 2: Comments on Guideline 1?			
Guideline	**Summary of responses received**	**EBA analysis**	**Amendments to the proposal**
1.7(a)	One respondent suggested that guidelines should require firms to update their business-wide risk assessment at a minimum once per calendar year.	The EBA notes that the comment refers to amendments which are not included or linked to the current consultation process. To clarify, according to the Guidelines, the firms should determine the need for updates on a risk-sensitive basis to ensure that the specific characteristics and business models are duly taken into consideration.	None
1.7(d) and	One respondent called for more clarity on what is meant by a 'delivery mechanism' in the context of CASPs' activities.	The EBA acknowledges that the reference to 'delivery mechanisms' might be confusing. Therefore, the EBA has replaced it with the term 'delivery channels' which is already used throughout the Guidelines.	1.7(d) and 21.3(e)

21.3(e)			
Feedback on responses to Question 3: Comments on Guideline 2?			
2.4(b)	One respondent asked the EBA to clarify the meaning of the term 'unregulated businesses' and whether it refers to companies that are regulated in a jurisdiction outside the EU or that do not require a licence in Europe. It is also unclear whether a company which is under a legal regime which only requires it to be registered and not regulated – as is the case for existing legal regimes in some EU Member States – would fall under this Guideline.	The term 'unregulated businesses' used in Guideline 2.4. b) should be read in connection with Guidelines 9.20 and 9.21., which explain how to determine if the business relationship is conducted with unregulated or regulated customers. The Guideline was amended to include a cross reference to Guideline 9.20.	2.4(b)
2.4(b)	Two respondents commented that the provisions may entail a due diligence process that is too onerous for CASPs to comply with, in particular, the requirement to identify risk factors associated with all non-EU countries and/or unregulated customers or beneficial owners with which they interact. Respondents suggested that the Guidelines should state that this risk factor should be subject to a risk-based approach rather than being set as a regulatory requirement.	Directive (EU) 2015/849 requires firms to know the risks associated with their customers, including their beneficial owners, and to take suitable measures to mitigate these risks. These Guidelines explain how firms can assess the risks and apply the CDD measures commensurate to those risks. Guideline 2.4(b) highlights one type of factor, which, if present, may expose the firm to an increased risk of ML/TF. However, the Guidelines are explicit that firms should take a holistic view of all risk factors to which their business or customers are exposed. This means that the customer's exposure to unregulated businesses or non-EU countries might not always lead to the customer being rated as high risk, if other risk-reducing factors are present.	None
Feedback on responses to Question 4: Do you have any comments on the proposed changes to Guideline 4?			
4.29	One respondent queried whether CASPs will only need to apply the measures listed in Guideline 4.29 a) and b) or would the entire document on EBA's Guidelines on the use of Remote Customer Onboarding Solutions be applicable to them.	In addition to complying with the EBA's Guidelines (EBA/GL/2022/15) on the use of Remote Customer Onboarding Solutions, credit and financial institutions should also apply provisions set out in a) and b) of Guideline 4.29.	None
4.35	One respondent asked the EBA to clarify the term 'relevant customer data', as this might in principle cover everything from the IP address to all the identification information and further guidance on how firms can ensure prompt access to data.	The term 'customer data' is used to describe all types of data necessary for the firm to identify and verify its customers in accordance with Article 13 of Directive (EU) 2015/849. Guideline 4 provides further guidance	None

		on the type of data that may be relevant. Furthermore, the EBA's Guidelines (EBA/GL/2022/15) on the use of Remote Customer Onboarding Solutions in paragraph 49 provide examples of customer data including, but not limited to, photography, videos and documents, during the remote onboarding process. Therefore, if an IP address is used by a firm to identify and verify the customer, firms obligations are the same as those applicable in respect of other data obtained during the CDD process.	
4.35	One respondent proposed that the Guidelines should also consider the data transfer and retention in case of termination of the relationship with the external provider, namely, the service agreement with the external provider should entail clauses for data management in case of termination of the agreement to assure data transmission is provided in a form that ensures integrity and uninterrupted accessibility.	The EBA agrees with the respondent that firms should put in place suitable controls to ensure that they are able to retrieve data from external providers at a time when the contract with them is terminated. The EBA has amended Guideline 4.35 to reflect the minimum standards applicable to firms in respect of outsourcing agreements. Furthermore, firms should also refer to the EBA's Guidelines on outsourcing arrangements (EBA/GL/2019/02), which provide further guidance on data transfers and retention. These Guidelines might also be useful to CASPs, although they might not be directly bound by them.	4.35
4.60 (a)	One respondent asked the EBA to provide more detailed guidance on how to identify 'successive transactions without obvious economic rationale' because, in the respondent's view, 'successive transactions without obvious economic rationale' do not themselves denote high-risk activity in the absence of other red flags. Another respondent explained that the triggers set out in Guideline 4.60 should not automatically justify or trigger enhanced CDD.	According to the Guidelines, the 'successive transactions without an obvious economic rationale' is only one example where the customer's transaction pattern 'differs from what the firm would normally expect' for this type of customer. This means that should the CASP, based on the customer's transaction history, expect the customer to request or process successive transactions, these transactions might not imply a high risk. To comply with this requirement, firms should compare the transaction with their customers' usual operational behaviour. The EBA has amended Guideline 4.60(a) to include examples of successive transactions which might be deemed unusual.	4.60 (a)
4.74(d)	Three respondents commented on the use of advanced analytics tools by CASPs, which, in their view, should be applied on a risk-sensitive basis, considering the nature, size, complexity of the business and the risk exposure of the customer. The respondents also suggested that guidelines should remain technologically neutral and should not prescribe the type of controls or tools that CASPs should implement.	In keeping with the risk-based approach, firms should determine the most appropriate controls and tools based on their business and risks associated with their business relationships. They should set this approach out in their policies and procedures. The risk-based approach is built into Guideline 4.74(d).	None

4.74(d)	One respondent suggested the inclusion of artificial intelligence (AI) solutions. This can serve as a reference for companies to stay abreast of the latest industry developments.	The EBA considers that the ability to use AI is already provided for in the Guidelines by the reference to 'advanced analytics tools'. The Guidelines require firms to decide on the most effective tools for their business.	None
Feedback on responses to Question 6: Do you have any comments on the proposed changes to Guideline 8?			
8.6(d) iii and 9.20	Four respondents raised concerns about the use of the term 'crypto-asset ecosystem' in Guidelines 8.6(d)ii and 9.20. In their view, the term is overly broad and has the potential to encompass a wide array of participants beyond the intended target, such as all crypto technology providers. As a result, banks may be reluctant to offer services to reputable entities that are not directly involved in CASPs' activities, but are part of the broader technology landscape that supports the crypto-asset sector.	The EBA agrees with the respondent that the reference to the 'crypto-assets ecosystem' may broaden the scope of providers. Both Guidelines refer to providers of crypto-assets services, which are not authorised as CASP's under Regulation (EU) 2023/1114, for example, providers established in non-EU countries. The EBA has amended both Guidelines, which now refer to 'providers of crypto-assets services, other than CASPs'.	8.6(d)iii 9.20
8.6(d)iii 8.8(d) and 21.3(d)ii	Five respondents asked for more guidance on how to assess the robustness of a non-EU country's AML/CFT regime. The respondents also enquired about the sources of information that should be used to make such an assessment as well as the assessment of geographical risks required in Guideline 8.8(d). According to the respondents, such an assessment may vary depending on the country being assessed and the approach taken by the regulators in such a country.	To assess the geographical risks associated with different jurisdictions, including the effectiveness of their AML/CFT regime, CASPs should refer to Guidelines 1.30 and 1.31 in Title I of the Guidelines in respect of sources of information and to Guidelines 2.9 - 2.15 in Title I, which explain the factors to be considered when assessing geographical risk. In particular, Guideline 2.11 provides examples of information sources that can be consulted when assessing the effectiveness of a jurisdiction's AML/CFT regime.	None
9.20	One respondent pointed out that the guidance does not currently specify which EU regulatory frameworks would be considered equivalent to Regulation (EU) 2023/1114 for the purposes of this guidance. In the respondent's view, the EBA should take into consideration that Regulation (EU) 2023/1114 at this stage only governs certain market participants (e.g. stablecoin issuers, CASPs), while other assets or providers that are either emerging, or fulfil different consumer demands are not subject to these requirements. Treating such entities as higher risk would therefore be premature as it would create undue burden for CASPs engaging in correspondent relationships.	It is important to note that Guideline 9.20 does not only refer to Regulation (EU) 2023/1114. There are different licensing regimes and registration requirements that entities have to undergo in order to provide financial services and therefore they are more supervised and regulated, including in the area of AML/CFT. Since the Guidelines follow the risk-based approach, the regulation and supervision decreases the customer risk, while the lack of such requirements increases it. The overall customer risk assessment will be the result of counterbalancing a number of customer, product, delivery channel and geographical risk factors. Refer also to our comments above in respect of Guideline 2.4(b).	None

8.6(d)iv **(also refer to GL 21.3(d))**	Eight respondents argued that transactions with self-hosted addresses should not be considered a risk-increasing factor and that CASPs allowing transfers to and from self-hosted addresses are always associated with higher levels of ML/TF risk. Some respondents suggested that there is no evidence to suggest that such transactions are associated with illicit activity and pointed out various benefits offered by self-hosted addresses to their users. Some respondents suggested that, as a result of this guidance, banks would be discouraged to enter into correspondent relationships with CASPs that interact with self-hosted addresses, which could lead to CASPs refraining from such business relationships.	The Guidelines recognise that transactions with self-hosted addresses are inherently higher risk than transactions between two CASPs due to the unregulated nature of these tools and, in particular, the lack of the identification and verification requirements applicable to the holders of self-hosted addresses. This means that any transactions with self-hosted addresses potentially present an increased risk for the CASP, particularly where they fail to provide the required information together with the transfer in accordance with Regulation (EU) 2023/1113. The EBA recognises that CASPs can implement systems and controls to mitigate these risks, which may reduce their residual risk exposure. However, the extent of this mitigation is determined by the effectiveness of the controls implemented by CASPs, which may differ from CASP to CASP.	None
8.6(d)iv	One respondent asked for further clarification on what business model is targeted by this provision that would result in an increased risk. Otherwise, the respondent suggested to delete the provision.	The Guideline refers to the risks presented by the respondent's business model and provides further guidance to firms on how they can meet their obligations under Article 19 of Directive (EU) 2015/849. The Guideline points at any business model which makes compliance with Article 19b of the Directive more difficult. The EBA acknowledges that the reference to self-hosted addresses in this Guideline is too limited and that the paragraph should instead refer to unregulated business models, as set out in Guideline 21.3 (d). The EBA has amended Guideline 8.6(d)iv to include a cross reference to Guideline 21.3(d)iv.	8.6(d)iv
8.6(h)	One respondent queried whether the change in the company's name or in its trademark is considered an indicator of an increasing risk under these Guidelines.	Guideline 8.6 h) refers to the risk when a respondent CASP provides an IBAN that is owned by another company (not the respondent's company) with which the respondent CASP does not have a business relationship, e.g. it is not owned by the CASP's subsidiary. Where the company is changing its name or its trademark, the correspondent should request the respondent CASP to provide registration documentation reflecting such changes. However, the name or the trademark change, in the absence of other risk-increasing factors, does not automatically increase the ML/TF risk rating of the customer. The EBA has amended the Guideline to clarify the ownership of the IBAN.	8.6(h)

8.8 (d)	One respondent asked for more clarity on what would constitute a 'sufficient level of certainty' when verifying the customer's jurisdiction and what level of attempt at verifying an IP address would sufficiently meet the requirements of the proposed Guideline.	In keeping with the risk-based approach, the Guidelines recognise that firms may not be able to determine the existence of certain risk factors to an absolute certainty. If, however, there are reasons to suspect or other factors pointing at an increased ML/TF risk, firms should intensify their efforts. As regards the level of verification of the IP address, firms are reminded that, according to the EBA's Remote Onboarding Guidelines, they are expected to apply controls to address risks associated with automatic capture of data. Such risks include, for example, the obfuscation of the location of the customer's device, spoofed IP addresses or services such as virtual private networks (VPNs). The EBA has amended the Guideline to clarify the verification mechanisms.	8.8(d)
8.17(a) and 8.17(c)	Three respondents raised questions on the practical application of this Guideline and in particular about the extent of measures that should be applied. They noted that non-EU/EEA CASPs are not required by law to disclose their AML/CFT controls and transaction monitoring tools where no business agreement exists between them and the EU CASP, therefore preventing the correspondent from meeting the obligations set out in these Guidelines. Also, while the EU CASP can ask about the respondent's monitoring tools in place, it is not possible for the CASP to assess whether they are appropriate. The respondents were concerned that should the provisions in Guideline 9.17 present a heavy burden and overheads for correspondent institutions, they might rather simply not engage in such correspondent relationships.	Where an EU/ EEA correspondent is engaging in a correspondent relationship with a non-EU respondent, their legal obligations are set out in Article 19 of Directive (EU) 2015/849. Guideline 8.17 provides further guidance on the steps the correspondent should take to identify risks associated with the respondent institution. To fulfil their legal obligations, the EU correspondents should do their utmost to gather the necessary information from the respondent when establishing the business relationship with it. In situations where the EU correspondent is unable to obtain the required information from the respondent, it may suggest an increased exposure to ML/TF risk. Sufficient measures to mitigate the risk, will depend, among other things, on the respondent's business model and its complexity, as well as the regulatory and supervisory framework applicable to the respondent. Should the risk exposure become too high and cannot be sufficiently mitigated, the EU respondent should consider whether it should continue the correspondent relationship. The adequacy assessment should be conducted using the risk-based approach. The depth of the assessment will therefore depend on the level of risks associated with the respondent and it should be determined according to these Guidelines.	None

Feedback on responses to Question 7: Do you have any comments on the proposed changes to Guideline 9?			
9.20	One respondent suggested that guidelines should encourage banks to cooperate with CASPs and not simply ban clients that fall into the CASP category. With only a few banks supportive of the crypto industry, this represents a major obstacle to further industry development, as well as further market adoption.	The EBA notes that the amendments to Guideline 9 already reflect the changes introduced by Regulation (EU) 2023/1114 and the inclusion of CASPs within the AML/CFT legal framework. Also, the Guideline has been strengthened to emphasise the need for banks to base their decision to enter or not to enter into a business relationship with a crypto-assets services provider, other than a CASP, on the ML/TF risk assessment, rather than on their perception of the risk presented by them. Furthermore, to reduce de-risking of certain types of customers by financial institutions, the EBA has published 'Guidelines (EBA/GL/2023/04) on policies and controls for the effective management of ML/TF risks when providing access to financial services firms'.	None
9.21(g)	One respondent noted that, while European entities are obligated to carry out checks listed in Guideline 9.21, non-European entities are not. This may have an adverse effect on the business of EU entities.	The EBA agrees with the respondent that the Guidelines do not apply, as such, to non-EU providers. However, should these providers wish to carry out their operations in the EU, e.g. by establishing an EU branch, they will also be obliged to comply with these Guidelines. Also, when a non-EU entity wishes to enter into a business relationship with an EU entity, its voluntary implementation of EU guidelines may be viewed as a risk-reducing factor.	None
Feedback on responses to Question 8: Do you have any comments on the proposed changes to Guidelines 10, 15 and 17?			
17.4	Two respondents queried why the funding of crowdfunding projects by crypto-assets may expose the crowdfunding service providers to an increased ML/TF risks, particularly where the crypto-assets are regulated by Regulation (EU) 2023/1114.	The EBA acknowledges that the ML/TF risk linked to transactions in crypto-assets has generally decreased due to the CASPs being regulated by the Regulation (EU) 2023/1114 and Regulation (EU) 2023/1113.Nonetheless, crypto-assets are still not fully equivalent to official currencies and not all crypto-assets are suitable to be used as payment instruments. Also, not all crypto-assets are within the scope of Regulation (EU) 2023/1114. As a consequence, the risk associated with those payments is increased. The EBA has amended Guideline 17.4 to reflect that not all crypto-assets may present the same level of risk. Refer also to our comment in respect of Guidelines 8.6(d)iii and 8.6(d)iv above.	17.4 (i) and 17.6(b)

Feedback on responses to Question 9: Do you have any comments on the proposed changes to Guideline 21?			
Guideline	**Summary of responses received**	**EBA analysis**	**Amendments to the proposal**
General comments	Two respondents commented on the scope of Guideline 21 and asked for the Guideline to clarify that risk factors need to be applied by CASPs on a case-by-case basis, considering CASPs' business and internal assessment of the risk factors. The Guidelines should not impose an excessive administrative burden on CASPs.	In accordance with Directive (EU) 2015/849, all obliged entities, including CASPs, are required to identify ML/TF risks associated with their business relationships and manage those risks through suitable CDD measures. With these Guidelines, the EBA guides CASPs on how to carry out this in practice. While the Guidelines provide an extensive list of various risk factors, CASPs should identify and assess those factors that are relevant for their business.	None
21.1	One respondent suggested that, in addition to general provisions on training in Guideline 6, the Guidelines should emphasise the need for specialised training for CASPs to develop an understanding of the technical aspects of crypto-assets.	The EBA agrees that appropriate training for relevant staff is crucial. The EBA has amended Guideline 21.11 to emphasise the need for specialised training.	21.11
21.2	Given that CASPs may offer more than one service, the respondent suggests that Guideline 21.2 should require that CASPs comply with other relevant guidelines in Title II.	The EBA agrees with the respondent and has amended Guideline 21.2 to highlight that, in certain circumstances, relevant sections in Title II may also be applicable to CASPs.	21.2
Products, services and transaction risk factors			
21.1 **21.3(a)** **21.5(b)xiv**	Two respondents' comment on the use of the privacy-enhancing tools. One respondent pointed out that the term 'privacy' is only mentioned in the context of privacy-enhancing measures, which are deemed conspicuous and trigger heightened risk profiles, without giving any consideration from a human-rights perspective. The other respondent argued that not all privacy-enhancing tools or features are the same and that they present varying levels of individual risk, which needs to be evaluated on a case-by-case basis.	Data privacy is addressed in the Article 25 of Regulation (EU) 2023/1113, which clarifies that processing of personal data under this Regulation is subject to Regulation (EU) 2016/679. The EBA, however, acknowledges the difference between 'privacy-enhancing features' and 'anonymity-enhancing features', considering that the latter presents higher ML/TF risks. Some examples of anonymity-enhancing features include, but are not limited to, mixers or tumblers, obfuscated ledger technology, ring signatures, stealth addresses, ring confidential transactions, atomic swaps, non-interactive zero-knowledge proofs and privacy coins. The EBA has amended Guidelines 21.1, 21.3(a) and	21.1, 21.3(a), 21.5(b)xiv

		21.5(b)xiv to emphasise the ML/TF risks associated with anonymity-enhancing features.	
21.3 (b)	Three respondents questioned the scope of Guideline 21.3(b). In particular, they asked to clarify whether the Guideline is referring to peer-to-peer crypto payments and crypto deposits, which are accepted by CASPs from unrelated third parties, potentially classifying most CASPs as high risk under this Guideline. They suggested that risks associated with these transactions can be effectively managed through the implementation of blockchain analysis tools and other controls.	Guideline 21.3(b) highlights the inherent risk associated with persons, other than customers, who are making payments on behalf of the customer, without an apparent economic rationale for it. The risk is presented by the fact that such persons are not known to the CASP as they have not been identified or verified. While the EBA agrees with the respondents that these risks can be mitigated via appropriate controls put in place by a CASP, the effectiveness of the mitigation would depend on the effectiveness of those controls. The EBA has amended Guideline 21.3(b) to clarify that the payment, from a person who has not been identified and verified at the outset by the CASP, may present an increased risk.	21.3(b)
21.3 (c)	Five respondents argued that CASPs are not exposed to increased ML/TF risks due to increased volumes or values of transactions, but rather how well these volumes/values are mitigated. The respondents are concerned that by identifying this as a risk factor, it may negatively impact crypto remittance products, as generally, CASPs don't put restrictions on the overall volume or value of transactions upfront, allowing funds to be moved swiftly.	The Guideline highlights that the level of ML/TF risk may be increased where the value or volume of transactions have not been restricted at a product level by a CASP. While the EBA recognises that residual risks may be mitigated by CASPs via the transaction monitoring systems and controls, the inherent risks presented by unrestricted movements of funds remain. The EBA has amended Guideline 21.3(c) to clarify that the risk may be increased where no upfront restrictions have been imposed.	21.3(c)
21.3(d)i	Five respondents disagree with the suggestion that self-hosted addresses are de facto considered to increase ML/TF risk of the CASP's customer. In the respondents' view, there does not seem to be any evidence supporting the high ML/TF risk exposure suggested by the Guidelines. One respondent referred to xpub (an extended public key), which allows CASPs to see all transactions and therefore, according to the respondent, the risk is reduced.	Please refer to the EBA's comment above in Guideline 8.6(d)iv.	None
21.3(d)i	Two respondents questioned whether these Guidelines impose any obligations on software developers because self-hosted addresses are solely software programs or interface software that allow a user to read blockchain data and compose transactions.	Self-hosted addresses are outside the scope of the AML/CFT legal framework, which means that these Guidelines do not impose any obligations on users of self-hosted addresses or developers of the necessary software. Self-hosted addresses are mentioned in the Guidelines due to potential risks they may present to CASPs, which are subject to	None

		these Guidelines.	
21.3(d)iv and 21.3(d)v (new Guide-lines 21.3(d)iii and 21.3(d)iv)	Seven respondents suggested that transactions between CASPs and DeFi trading protocols/platforms or peer-to-peer crypto-asset exchange platforms should not be considered a risk-increasing factor. The respondents noted that in the current environment, it is not possible for CASPs to engage directly with DeFi protocols, meaning that a reference to CASPs' transactions with DeFi in Guideline 21.3 would have a limited effect. The respondents also pointed out that such platforms do not present the same level of risk as mixers or tumblers.	The Guidelines recognise that transactions with peer-to-peer platforms and DeFi trading protocols/platforms may present an increased risk for CASPs due to the lack of legal framework applicable to these platforms and the absence of legal obligations to identify and verify their users. The EBA recognises that peer-to-peer platforms possess similar characteristics and risks as DeFi protocols/platforms, therefore, the EBA has merged provisions in Guidelines 21.3(d)v. and 21.3(d)iv under a new Guideline 21.3(d)iii. While the EBA recognises that, due to technical limitations, CASPs may rarely interact with DeFi trading protocols/platforms, when such transactions happen, CASPs should be aware of the risks to which they may be exposed. Furthermore, the EBA agrees with the respondent that the characteristics of mixers and tumblers differ from those of peer-to-peer and DeFi trading protocols/platforms, and therefore have separated those provisions in a new Guideline 21.3(d)iv.	21.3(d)iii and 21.3(d)iv
21.3(d)vi (new GL 21.3(d)v.)	One respondent asked for further details on what is meant by 'other hardware' in the Guideline, as this formulation may lead to a wide scope of potential hardware devices being captured by the Guideline	A reference to the 'hardware' here means any hardware used to exchange crypto-assets to official currencies and vice versa. The EBA amended Guideline 21.3(d)v to clarify this.	21.3(d)v
21.3(e)	Three respondents asked the EBA to clarify what is meant by the 'ML/TF risk, which is not yet fully understood by the CASP' and at what point or after how long it is considered that the risk is well understood. The respondents also questioned whether the inclusions of this risk factor in the Guidelines may not lead to every new product involving new business practices being considered high risk.	The meaning of the term 'fully understood' is linked to the CASP's ability to reliably assess the ML/TF risk associated with new business practices, e.g. due to the lack of use cases or reliable data. Furthermore, the EBA is of the view that the inclusion of a timeline may not be detrimental for CASPs, because it could go beyond the time actually needed by CASPs to assess the ML/TF risk of a new technology or new practices. The EBA has amended Guideline 21.3(e) to replace the reference to 'fully understood' with 'cannot be reliably assessed'.	21.3(e)

21.3(f)	One respondent explained that such a risk factor is also relevant in other sectors, as there are many intermediary financial service providers that offer nested services, for example, fund managers and alternative fund managers.	The EBA agrees that the risk factor may also be relevant in other sectors, however, it is explicitly set out in this Guideline to emphasise its importance for CASPs in relevant situations also.	None
21.3(g)	One respondent suggested also including the 'results of an analysis ran by advanced analytics tools' as a higher ML/TF risk indicator.	The EBA points out that, as a general principle, CDD measures should be proportionally intensified in cases where ongoing monitoring indicates an increased ML/TF risk, regardless of the tools used to monitor transactions. Nonetheless, the EBA acknowledges that the focus on advanced analytics tools is more relevant for CASPs.	21.3(g)
21.4 (b)(iii)	One respondent commented that this risk mitigating factor may potentially be used by CASPs as a key factor when rating the customer as low risk, based on the assumption that the bank holding the account will manage the risk.	The Guidelines are clear that, in order to perform a risk assessment that is effective and meaningful, firms, including CASPs, should identify and assess all relevant risks associated with their business and customers in a holistic way (refer to Guideline 3.2 in Title 1 of the Guidelines). This also applies to risk-reducing factors, which means that one factor cannot determine the overall risk exposure of the customer or transaction.	None
21.4 (d)	One respondent asked for clarification on whether this risk factor refers to the testing of a product, such as a pilot. According to the respondent, a product that is only available to certain categories of customers does not automatically classify it as low risk, but the level of risk ultimately depends on the type of customer and product.	These risk factors are put in place to help CASPs to determine the risk profile of the product and a customer. This risk factor addresses a specific situation where a product is offered only to a specific type or a closed loop of customers that are deemed low risk. The EBA has amended Guideline 21.4(d) to clarify the meaning of 'closed loop'.	21.4(d)
21.4	One respondent suggested also including 'a non-custodial wallet proven to be under the control or ownership of a CASP's customer as a risk-reducing factor'.	The EBA recognises that the ownership or controls of a self-hosted address by the CASP's customer may provide a level of assurance for the CASP that the risk associated with transactions to/from that self-hosted address may be mitigated to a certain extent. The EBA has amended Guideline 21.12 to incorporate an additional risk mitigating measure 21.12(m) into the Guideline.	21.12(m)
Customer risk factors			

21.5(a)iii	One respondent suggested that the type of company and business model of the company should also be taken into consideration in this risk factor. A company that is new and processes a large transaction volume does not necessarily mean it is risky.	The EBA acknowledges that it is not the case that the recent establishment of a company or having a large volume of transactions implies high risk in all cases. This risk factor aims to capture those situations where a new business may have been created specifically to facilitate money laundering and terrorist financing. Indeed, the business model is relevant, but it is already included as a factor in (among others) 21.5(a)(ii), 21.5(a)(iv) and 21.5(a)(v) and in Title I of the Guidelines.	None
21.5(a)v.	Five respondents asked for further guidance on what is considered 'an intra-group relationship' in the context of the crypto-asset sector. Respondents are concerned that, because of the interconnectedness of blockchain infrastructure, this term could plausibly include almost every crypto company. In the respondents' view, as long as sound disclosure requirements are in place, this scenario would not inherently be riskier than others.	The EBA notes that the 'group' is defined in Article 3(15) of Directive (EU) 2015/849. The Guideline highlights the possible risk arising from a potentially unfair reliance on the CASP's own group practices The EBA has amended Guideline 21.5(a)v to clarify that only groups as defined in the Directive are captured by this Guideline.	21.5(a)v.
21.5 a) vi.	One respondent commented that the use of anonymous or randomly generated email addresses increases the anonymity of a customer and that the same applies to customers using temporary email services.	The EBA agrees with the respondent and have amended Guideline 21.5(a)vi to include the use of temporary email addresses as a potential risk-increasing factor.	21.5(a)vi
21.5(a)vii and 21.12(k)	Two respondents asked for further guidance on how CASPs can assess the vulnerability or the lack of knowledge of crypto-assets by a customer required by Guideline 21.5(a)vii, especially if the onboarding process already includes an appropriateness and knowledge test.	The report published by the FATF in February 2023 on Countering Ransomware Financing provides multiple examples of situations where money mules are used by criminal groups in the laundering process. In particular, when exchanging crypto-assets into official currencies. The report describes that 'money mules have no internet presence and have little internet literacy'. The EBA agrees that the appropriateness/knowledge test may help to identify such persons; however the CASPs are reminded to be alert to any other signs suggesting that a customer may be a used as a money mule. The EBA has amended Guideline 21.5(a)vii to provide further guidance on how CASPs can identify such customers.	21.5(a)vii
21.5 (b) i.	One respondent suggested that when a customer tries to open multiple crypto-asset accounts with the CASP and/or creates separate accounts under different names to circumvent restrictions on trading or withdrawal limits imposed by CASPs, such a customer may also present an increased risk.'	The EBA agrees with the respondent that the proposed situation may present an increased ML/TF risk and has amended Guideline 21.5(b)i to reflect this.	21.5(b)i

21.5 (b) (ii) (b)	One respondent commented that the use of money transmitters can be seen as an increasing ML/TF risk, especially if the money transmitters cannot produce the required CDD information and documentation.	The EBA agrees that money remittance services may present an increased risk in some situations, in particular those not falling within the remit of Article 11(b)(2) of Directive (EU) 2015/849; however this risk factor is already addressed in Guideline 2.4(b) in Title I of the Guidelines. The aim of Guideline 21.5(b)ii(b) is to highlight the risk associated with different tools that may be used to hide the identity of the beneficial owner.	None
21.5(b)ii (c)	One respondent pointed out that there is no obligation on CASPs to query the purpose of each transaction. Therefore, the Guideline should envisage that the purpose would be queried only in those cases where the surveillance team has flagged a transaction that is not in line with the customer's profile.	The EBA would like to clarify that the Guideline aims to highlight situations whereby the information is requested by a CASP, but not provided by the customer. The EBA has amended Guideline 21.5(b)ii(c) to clarify this.	21.5(b)ii(c)
21.5(b)v	One respondent asked to clarify what is meant by 'appears to belong to a group of individuals that conduct their transactions at a single or multiple outlet or location or across multiple services' in Guideline 21.5(b)v.	The risk factor aims to identify customers who may belong to a criminal group. The identification of this risk factor is not mutually exclusive from the CASPs' reporting obligations under Article 33 of Directive (EU) 2015/849. The EBA has amended Guideline 21.5(b)v.	21.5(b)v
21.5(b)vii	One respondent suggested that the Guidelines should include a reference to 'by frequent transfers of unusual amounts of crypto-assets to avoid the risk of ordinary transactions being flagged as high risk.'	The Guideline addresses situations whereby a customer is regularly receiving or making transfers in respect of such amounts that are just below the threshold, which may suggest the intention to avoid the verification of the beneficiary or the originator in accordance with Article 14(5) or Article 16(2) of Regulation (EU) 2023/1113. The reference to 'unusual amounts' is not relevant in this Guideline. The EBA has amended Guideline 21.5(b)vii to provide further explanation that the risk factor aims to address 'frequent transfers' below the threshold triggering the verification of the originator.	21.5(b)vii
21.5(b)vii i	One respondent explained that an investment in an initial coin offering or a product offering a high return is not necessarily correlated with an increased risk of ML. Rather, it correlates to the risk appetite of a customer.	The Guideline highlights potential risks associated with initial coin offerings, which offer disproportionately high returns and where they are linked to fraud-related indications or high-risk jurisdictions. The EBA has amended Guideline 21.5(b)viii to clarify this.	21.5(b)viii
21.5(b)ix (a)	One respondent indicated that the situation identified in this Guideline could be an indicator of an account takeover and the customer would be contacted to verify whether the customer is performing the transaction in question.	The action described is what would be expected from the CASP in response to a sudden increased activity, so as to determine whether there is an explanation or otherwise for any such change. The reference to	None

		'unexpected and without any reason' refers to a situation where the customer could not provide a reasonable explanation for the transaction.	
21.5(b)ix (c)	One respondent explained that CASPs would generally ask questions about the customer's income. In particular, if the deposit volume significantly exceeds the anticipated deposit volume or if it exceeds the income that they have stated, then such a situation would require further investigation.	The EBA agrees with the respondent. The EBA has amended Guideline 21.5(b)ix(c) to emphasise the link between the transaction limits and the customer's declared income.	21.5(b)ix(c)
21.5(b)x	One respondent suggested that the conclusions about the level of risk should be based on the customers' business model and their activities, rather than their transactions with multiple jurisdictions. If transactions with different jurisdictions is something new that the customer did not do in the past, then such behaviour should be closely monitored to determine the reasons behind this new behaviour.	The intention of these Guidelines is to address unexplained or unjustifiable behaviours. Should there be a reasonable explanation for the transfers, then the transactional pattern in itself may not be a high-risk factor. Although there might be other factors related to the transactions that may suggest an increased ML/FT risk. However, the decision that the transaction pattern does not present an increased risk cannot be dependent only on the customer's past transaction activities. It has to be supported by a reasonable explanation as to why this customer behaviour is acceptable. The EBA has amended Guideline 21.5(b)x to emphasise that unexplained transfers may present an increased risk.	21.5(b)x
21.5(b)xi(a)	One respondent emphasised that the use of multiple credit cards by a customer is not an indication of a risk, as it is common for multiple disposable credit cards to be used to increase the safety when shopping online.	The use of multiple payment methods, be they of the same kind or otherwise, allows the obfuscation of an audit trail. This is just one factor to be considered when determining the overall ML/FT risk profile of a business relationship, as there may be other factors that may lower the said ML/FT risk.	None
21. 5 (b)xi	One respondent suggested that a situation where a customer deposit crypto-assets at an exchange and then immediately withdraws them from a CASP to a private wallet may also present an increased risk.	The EBA agrees with the respondent and has added a new Guideline 21.5(b)xi(h).	21.5(b)xi(h)
21.5(b)xiii	One respondent highlighted that in situations where the source of the crypto-asset is associated with the darknet or illegal/high-risk sources, the customer's behaviour could indicate higher ML/TF risk.	The EBA agrees with the respondent and has amended Guideline 21.5(b)xiii to highlight risks associated with crypto-assets linked with the darknet.	21.5(b)xiii
21.5 (b)(xii)	One respondent explained that where the customer is investing crypto-assets borrowed on a peer-to-peer lending platform, it may	The risk does not stem from the fact that the customer is investing borrowed crypto-assets but from the source of the said assets. In particular,	None

	be an indication of a high investment risk appetite, rather than higher risk exposure of the customer.	the lack of oversight by the lending platform over the lender is increasing the risk that the borrowed crypto-assets may be linked to illegitimate sources or a criminal activity. Refer also to the response on Guideline 21.3(d)iv above.	
21.5 (b)(xiii)	One respondent asked to clarify that the provision excludes tokens that have been cleared of their association with criminal activities (for example, after being confiscated and auctioned off by law enforcement).	Any information on the subsequent clearing of any tainted crypto-assets may be considered as part of CASP's monitoring activities of a business relationship with the customer.	None
21.5 (b)(xv)(b)	Four respondents explained that the use of multiple self-hosted addresses or multiple addresses located in different CASPs may be legitimate behaviour and, in some cases, considered a good practice. If a company has the xPub address from the client, as this is the main address that generates all wallet addresses, the company will be able to see all addresses belonging to the customer.	While not excluding the fact that there may be justifiable reasons for using multiple self-hosted addresses, the inability to clearly associate them with their users and identify and verify these users, leaves them open to abuse. Furthermore, the risk factor refers to the use of multiple self-hosted addresses, which increases the ML/FT risk significantly, especially if there is no reasonable justification for it. Refer also to our comments on the use of self-hosted addresses above.	None
21.5(b)xv (c)	One respondent suggested that the Guideline should also consider previously inactive accounts, which could be used for fraud or for ML/TF purposes.	The EBA agrees with the respondent that the use of previously inactive accounts may present an increased risk of ML/TF and has amended Guideline 21.5(b)xv(c) to reflect this.	21.5(b)xv(c)
21.5(b)xv (e)	Two respondents explained that some customers may prefer to keep their crypto-assets in a self-hosted wallet, instead of keeping them with the CASP as they might not wish to trade it immediately. The respondents questioned whether companies that receive crypto-assets in batches regularly to settle payments and convert them into official currencies on a short-term basis should be considered a high-risk businesses under this Guideline.	The intention of the Guideline is to highlight the ML/FT risk inherent in situations where crypto-assets are transferred to a service provider, only for the same crypto-assets to then be transferred to a self-hosted address without any economic rationale for such a transfer. These situations increase the risk that the CASP may be used in a layering context. The EBA has amended the Guideline to explain that the behaviour described in Guideline 21.5(b)xv(e.) may present an increased risk where there is no apparent economic rationale for such withdrawals or transfers.	21.5(b)xv(e)
21.5(b)xv (f)	One respondent explained that, based on their experience, users often transfer amounts under EUR 1 000 because they only trade small amounts, and not because they want to avoid travel rule restrictions.	The Guideline refers to repeated and frequent transfers of this nature. In addition, it is not every amount below EUR 1 000 that would increase risk but where a number of transactions are close to the said threshold.	None

21.5 (b)xv(h)	One respondent suggested adding an additional risk factor that refers to the customer's different crypto-asset accounts or distributed ledger addresses held by the same or different CASPs.	The EBA agrees with the respondent and has included a new Guideline 21.5(b)xv(h) as proposed by the respondent.	21.5(b)xv(h)
21.5(b)xvi	One respondent questioned how CASPs can identify such exploitation of glitches, as it would only be noticed once the behaviour has happened. The respondent provided an example of 'a double spend attempt' as an example of a technical glitch.	The purpose of the Guidelines is to highlight to the CASPs that the ML/FT risk of the relationship or of the transaction could be increased where they identify situations of this happening or having happened in the past.	None
21.5(b)xvii (new GL)	One respondent explained that transactions in crypto-assets involve a transaction fee, which is proportionate to the amount of computation or storage required to perform the transaction. Where the customer is claiming that a crypto-asset was obtained through mining or staking rewards, while transaction fees being significantly disproportionate to the transferred asset's value, may present an increased risk. In such cases, the miner or staker may fabricate an excessively high transaction fee to launder money.	The EBA agrees with the respondent that such situations may present an increased risk to CASPs. The EBA has included a new guideline to reflect risks associated with disproportionate fees involved in mining or staking.	21.5(b)xvii
21.6 (e)	One respondent asked to remove the reference to 'lawful merchants and service providers' in this provision as CASPs that are exchanging crypto-assets will not have a customer relationship with such merchants. CASPs therefore are unable to assess their lawfulness.	The EBA acknowledges that the CASP may not be able to assess whether a merchant or a service provider is lawful. However, the CASP should be able to assess if there are any concerns associated with the crypto-asset account or the distributed ledger addresses through the use of analytical tools deployed by CASPs. The EBA has amended Guideline 21.(e) to explain that the absence of 'adverse information' may be considered as a risk-reducing factor.	21.6(e.)
21.6(f)	One respondent suggested including an additional risk-reducing factor where the customer is in an intra-group relationship where both companies are regulated.	The EBA agrees with the respondent that crypto-asset transfers between two CASPs regulated under Regulation (EU) 2023/1114 reduces the risk, regardless of whether or not the CASPs are in the intra-group relationship. The EBA has included a new Guideline 21.6(f) to reflect the reduced risk presented by transfers between two regulated CASPs.	21.6(f)
Country or geographical risk factors			
21.7(a) and	Two respondents commented on the use of the term 'links' in these Guidelines and asked to clarify what such links should represent and how such information can be obtained in practice.	Both Guidelines identify situations in which a CASP is exposed to an increased risk associated with high-risk jurisdictions. CASPs should refer to	21.7(a) and 21.7(c.)

21.7(c.)		Guidelines 5.53-5.57 in Title I of the Guidelines for more details on how they can identify and assess this risk. The EBA has amended Guidelines 21.7(a) and 21.7(c) to align the terminology with that used in Title I and has replaced the term 'links' with 'involving high-risk non-EU countries'.	
21.7(d)	One respondent questioned why the Guideline excludes the EU countries. The respondent referred to the FATF rating of some EU countries as being a high-risk non-compliant jurisdiction for ML.	When evaluating whether a jurisdiction is associated with a high risk of ML/TF or predicate offences, CASPs should refer to Guidelines 2.05-2.15 in Title I of the Guidelines. The EBA has amended the Guideline to clarify that the geographical risks associated with different jurisdictions should be assessed in keeping with these Guidelines.	21.7(d)
21.7 (d) and 21.8 (a)	One respondent questioned the reference to predicate offences in these Guidelines as it could lead to a disproportionately negative impact on the assessment of ML/TF risk. This is due to variations in what is considered a predicate offence in different jurisdictions. For instance, a country that considers all crimes as predicate offences might report a higher number of offences compared to another that only considers serious crimes as predicate offences.	Guideline 2.15 in Title I of the Guidelines provides guidance on how CASPs can determine the level of predicate offences in different jurisdictions as part of their risk assessment and the information sources they can consult as part of this. Therefore, the EBA has amended Guideline 21.7(d) to remove a reference to predicate offences. In Guideline 21.8(a), the EBA has replaced a reference to 'predicate offences' with a reference to 'low levels of the ML/TF risk'.	21.7(d) 21.8(a)
21.7(e.)	According to one respondent, this Guideline implies that if a company, as a result of its monitoring, identifies that a customer is in a relationship with a third party involved in mining in a jurisdiction that is subject to international financial sanctions (e.g. Russia, Venezuela), the customer is considered to be in a relationship with a sanctioned entity. The respondent questioned why the focus is specifically on mining and not on other activities.	The Guideline recognises that both direct and indirect exposures to sanctioned jurisdictions may have an impact on the ML/TF risk of the customer. However, it should be determined by the CASP which indirect exposures have a material impact on the customer's the ML/TF risk exposure.	None
Distribution channel risk factors			
21.9(c.)	One respondent disagreed with the provision that all business relationships between CASPs and their customers that are established through an intermediary service provider in the crypto-assets ecosystem outside the EU are inherently higher risk.	According to the risk-based approach, any intermediary which is not regulated or not regulated in the EU, is considered to present an increased ML/TF risk. However, the CASPs should assess all relevant risk factors, including whether the intermediary performs CDD, to determine whether such a delivery channel presents a high risk. The EBA has amended Guideline 21.9(c) to include a cross reference to Guideline 9.20.	21.9(c.)

21.9(d)	One respondent was unclear how a CASP could verify or know from another party that the service provider gathers information in a high-risk jurisdiction or is using an outsourcing service provider located in a high-risk jurisdiction.	The Guideline highlights risks, which may arise in situations where a CASP enters into an outsourcing arrangement with a provider based in a high-risk jurisdiction and where that provider is to carry out the identification and verification of the CASP's customers. In such cases, CASPs are reminded that they are responsible for compliance with the AML/CFT obligations. The CASP is expected to have appropriate oversight procedures in place to assess the services carried out by the outsourced services provider. The EBA has amended the Guidelines to clarify this point.	21.9(d)
21.9(e.)	Three respondents suggested that the Guideline implies that any new or innovative distribution channels or new technology used for crypto-asset distribution, without prior full testing or usage, should be automatically categorised as high risk. In the respondents' view, such tools or channels do not necessarily carry a higher risk, especially when they have undergone the necessary auditing and testing process.	In accordance with Guideline 1.79(d) in Title I of the Guidelines, all CASPs are required to assess new products, including new distribution channels, before their launch. If the assessment shows that the distribution channel increases the CASP's exposure to ML/TF risks, the CASP should implement appropriate measures to mitigate these risks. For example, the CASP may apply more intense monitoring of the business relationship onboarded via that channel. Similar considerations also apply to the use of new technology, which is not fully tested, as it may expose the CASP to higher ML/TF risks. The EBA has amended Guideline 21.9(e.) to include references to those technologies or distribution channels that may present a high ML/TF risk.	21.9(e.)
Measures – Enhanced customer due diligence			
21.11 and 21.13	Three respondents pointed out that advanced analytics tools can also fail, like any other monitoring tool, and are not a panacea. In the respondents' view, CASPs should have suitable monitoring tools in place, but the tools chosen for such monitoring should be decided by the CASP.	On the use of advanced analytics tools, refer to our comments in respect of Guideline 4.74(d) above. The EBA has amended Guideline 21.11 to emphasise the CASP's obligation to implement appropriate and effective monitoring tools.	21.11
21.12	One respondent noted that carrying out open source or adverse media searches, as well as commissioning a third-party intelligence report to comply with the provisions laid out in Guideline 21.12 could be extremely onerous on CASPs, especially when dealing with a high volume of transactions.	Guideline 21.12 sets out a list of measures which could be applied by CASPs, however, not all measures may be necessary in all cases. CASPs should determine the right type and level of measures, based on the level of ML/TF risks presented by the business relationship. The EBA has amended Guideline 21.12 to emphasise that measures set out in the Guideline should be applied as deemed necessary by CASPs based on	21.12

		their risk rating of business relationships.	
21.12 (d)ii and 21.12(d)ii i	Three respondents commented that some measures appear to be significantly more detailed and prescriptive than those applicable to a broader range of financial institutions. In particular, the respondent suggested that provisions in Guidelines 21.12(d)(ii) and 21.12 (d) (iii) go beyond the requirements set out in the Regulation (EU) 2023/1113.	In accordance with Article 13 of Directive (EU) 2015/849, CASPs are required to gather information about the source of funds and source of wealth where deemed necessary in higher risk situations. Such a determination should be based on a holistic assessment of all relevant risk factors. Therefore, the EBA acknowledges that provisions in points i, ii and iii of Guideline 21.12(d) may appear to be too prescriptive. The EBA has amended Guideline 21.12(d) and has removed the sub-sections.	21.12(d)
21.12 (a)	One respondent commented that the identification and verification of CASPs' customers should contain additional measures compared to other industries, as CASPs usually conduct non-face-to-face business relationships with their customers and online business relationships offer a certain level of anonymity. The respondent suggested including in the Guideline examples of such CDD measures like IP addresses with an associated time stamp, geolocation data, device identifiers, wallet addresses and transaction hashes.	While the EBA recognises that additional tools and measures may be applied by CASPs to identify and verify their customers, the Guidelines aim to provide flexibility for CASPs to determine the most appropriate CDD measures for their business and type of customers.	None
21.12(b)	One respondent questioned whether the Guideline requires CASPs to identify and verify majority shareholders that do not meet the ultimate beneficial owner (UBO) definition.	The identification and verification of majority shareholders is an example of the type of enhanced CDD measures that may be applied in certain circumstances, as determined by the CASP.	None
21.12(c.) v	One respondent suggested that the reference to 'individuals who may influence the customer's operations' should be removed from the Guidelines. The management board members are identified as well as UBOs, thus the respondent considers the Guideline to be too broad, as it may encompass all potential 'individuals who may influence its operations' without these individuals posing any significant level of ML/TF risk.	The Guideline aims to raise CASPs' awareness of potential ML/TF risks associated with individuals who might not hold an official position within the customer's institution but who might exercise a significant influence on the customer's business due to, e.g. their previous position in the company or close family ties to other individuals in the company. The EBA notes that the identification of such individuals might be relevant in higher-risk situations and where the CASP is aware of such individuals, e.g. from media reports or other sources. The EBA has amended Guideline 21.1(c)v to address such individuals who are known to exercise significant influence on the business of the customer.	21.12(c)v

21.12(c)vi	One respondent queried the use of the term 'trading history' and whether the Guidelines require CASPs to obtain evidence of the source of crypto-assets or if the scope is more general. If the intention is to gather the customer's trading history outside the CASP system, then, according to the respondent, the measure will not be adopted in practice due to its high level of intrusiveness.	The EBA clarifies that the reference to the trading history refers to transactions from within the CASP's system. The gathering of such information depends on the respective business activity of the costumer, e.g. it might be relevant where the customer is a CASP. The EBA has amended Guideline 21.12(c)vi to further clarify this point.	21.12(c)vi
21.13	Two respondents questioned why the Guidelines imply that enhanced CDD measures should always be applied by CASPs when transacting with self-hosted addresses.	According to the risk-based approach, more CDD measures should be applied to those business relationships that present the highest ML/TF risk. Refer also to our comments in respect of Guideline 8.6(d)iv above where we have explained the risk associated with transfers involving self-hosted addresses and our rationale for it.	None
21.12(d)	One respondent advised that CASPs determine the source of income and the source of wealth of their customers not necessarily per transaction, but per customer.	The measures listed in Guideline 21.12 (d) are applicable in those cases where the CASP is carrying out the plausibility checks on potentially suspicious transactions or transactions that are deemed high risk. The EBA has amended Guideline 21.12(d) to clarify that this measure is not applicable in respect of all transactions, but only those that are potentially suspicious or present high ML/TF risk.	21.12(d)
21.12(i)	One respondent explained that it was impossible for a CASP to know whether the customer has addresses in multiple distributed ledgers or blockchain networks, unless the customer reveals them or transacts from those addresses with the CASP. In such cases, the CASP would take a note, record this information and associate it with the customer.	Through the use of advanced analytics tools, a CASP can determine whether the customer has one or multiple distributed ledger addresses. The application of this measure may be relevant in such cases where the customer's transactions have raised some suspicions or concerns.	None
Measures – Simplified customer due diligence			
21.15	One respondent questioned why the Guidelines disproportionately restrict simplified CDD options for CASPs. Notably, none of the proposed options permit more lenient identification or verification standards for individuals, and the reduction in monitoring scope is confined solely to specific products with recurring transactions.	According to the Guidelines, CASPs are responsible for identifying low-risk relationships in which simplified CDD measures would provide them with sufficient information about the customer. The Guidelines in 21.15 only provide examples of those simplified CDD measures, however the CASPs are not prevented from identifying additional measures which would allow them to sufficiently fulfil their obligations under Article 13 of Directive (EU) 2015/849.	None

21.15(a)	One respondent suggested that guidelines should allow simplified CDD to be applied to those customers who are engaged in businesses relating to crypto-assets and which have been licensed for many years.	The EBA notes that there is no such provision in the other financial sectors and, considering the risk-based approach, it would not be appropriate to include it for CASPs. It is important to stress that by having a licence for several years, in the absence of other risk-reducing factors, does not automatically indicate a low-risk situation.	None
21.16	Two respondents commented on the record keeping provisions in this Guideline. One respondent noted that it is not currently the practice for CASPs to copy the outcomes/information that they see in the blockchain. The respondent asked for more clarity on whether CASPs need to store the exposure of any transactions based on transaction hashes and a backup of this information and the length of time this information should cover. The other respondent asked the EBA to explain why reliance on distributed ledger for recordkeeping is not sufficient.	It is necessary for CASPs to have sufficient information about a transaction to perform the transaction monitoring and eventually report a suspicious transaction to the Financial Intelligence Unit (FIU). All information, which is necessary for such a report, must therefore be kept by the CASP. Reliance only on blockchain is not sufficient, as it is necessary to associate the wallet address with the customer or a person that controls the private key. The EBA has amended Guideline 21.16 clarifying that additional recordkeeping processes should be implemented by CASPs.	21.16