EBA/GL/2024/11

04/07/2024

Final Report

Guidelines

on information requirements in relation to transfers of funds and certain crypto-assets transfers under Regulation (EU) 2023/1113

(‘Travel Rule Guidelines’)

Contents

1. Executive Summary

Regulation (EU) 2023/1113 on information accompanying transfers of funds and certain crypto-assets was published on 9 June 2023. It recasts Regulation (EU) 2015/847 and extends its scope to the transfer of certain crypto-assets. Its main objective is to make the abuse of funds and certain crypto-asset transfers for terrorist financing and other financial crime purposes more difficult, and to enable relevant authorities to fully trace such transfers where this is necessary to prevent, detect or investigate money laundering and terrorism financing (ML/TF).

Regulation (EU) 2023/1113 does not set out in detail what payment service providers (PSPs), intermediary PSPs (IPSPs), crypto-asset service providers (CASPs), and intermediary CASPs (ICASPs) should do in order to comply with it. Instead, it mandates the European Banking Authority (EBA) to issue guidelines to PSPs, IPSPs, CASPs, and ICASPs on the steps they should take to detect missing or incomplete information that accompanies a transfer of funds or crypto-assets, and the procedures they should put in place to manage a transfer of funds or a transfer of crypto-assets lacking the required information.

The EBA delivers the mandates by repealing the 2017 Joint European Supervisory Authorities (ESAs) *Guidelines under Article 25 of Regulation (EU) 2015/847 on the measures payment service providers should take to detect missing or incomplete information on the payer or the payee, and the procedures they should put in place to manage a transfer of funds lacking the required information*[1]. The risk-based approach put in place by the ESAs at the time sets clear regulatory and supervisory expectations while leaving sufficient room for PSPs, IPSPs, and now CASPs and ICASPs, to define their approach in a way that is proportionate to the nature and size of their business, and commensurate with the ML/TF risk to which they are exposed. It therefore remains relevant and has been maintained in the final report.

Competent authorities will refer to these Guidelines when assessing whether the procedures PSPs, IPSPs, CASPs and ICASPs have put in place to comply with Regulation (EU) 2023/1113, are adequate and effective.

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 two months after the publication of the translations. The Guidelines will apply from 30 December 2024.

[1] JC/GL/2017/16.

2. Background and rationale

Background

On 26 June 2015, Regulation (EU) 2015/847 on information accompanying transfers of funds entered into force. This Regulation aimed, inter alia, to bring European legislation in line with Recommendation 16 of the *International Standards on Combating Money Laundering and the Financing of Terrorism and Proliferation*, which the Financial Action Task Force (FATF) adopted in 2012. Regulation (EU) 2015/847 specified which information on the payer and the payee must be attached to funds transfers by the PSPs – the so-called 'travel rule'. It also required PSPs to put in place effective procedures to detect the transfer of funds lacking this information, and to determine whether to execute, reject or suspend such transfers. The objective was to prevent the abuse of funds transfers for terrorist financing and other financial crime purposes, to detect such abuse should it occur, to support the implementation of restrictive measures, and to allow relevant authorities to promptly access the information. In line with the mandate, the ESAs issued Guidelines JC/GL/2017/16 on the steps PSPs should take to comply with that Regulation.

Since the adoption of Regulation (EU) 2015/847, the FATF has extended the application of Recommendation 16 to virtual asset service providers. This was because, in the FATF's view, the transfer of virtual assets gives rise to ML/TF risks.

In July 2023, Regulation (EU) 2023/1113 came into force and recast Regulation (EU) 2015/847, extending it to transfers of crypto-assets. It also extends the definition of 'financial institution' in Directive (EU) 2015/849 to CASPs that are regulated in accordance with Regulation (EU) 2023/1114. This means that once Regulation (EU) 2023/1113 applies, CASPs will be subject to the same AML/CFT system and control requirements as other credit and financial institutions within the scope of Directive (EU) 2015/849.

Article 36 (first and second subparagraphs) of Regulation (EU) 2023/1113 and Article 19a(2) of Directive (EU) 2015/849 require the EBA to issue guidelines to PSPs, IPSPs, CASPs and ICASPs on the measures they should take to detect missing or incomplete information on the payer or the payee, and the procedures they should put in place to manage a transfer of funds or crypto-assets lacking the required information.

The EBA publicly consulted on a draft version of these Guidelines between 24 November 2023 and 26 February 2024. A public hearing took place on 17 January 2024. Thirty-three respondents provided comments, which the EBA considered when preparing the final version of these Guidelines. These Guidelines repeal Guidelines JC/GL/2017/16.

Rationale

Through these Guidelines, the EBA promotes the development of a common understanding by PSPs, IPSPs, CASPs and ICASPs and competent authorities across the EU, of effective procedures to detect and manage the transfer of funds and crypto-assets lacking the required information on the payer/originator and the payee/beneficiary, and how these procedures should be applied. A common understanding is essential to ensure the consistent application of EU law. It is also conducive to a stronger EU AML/CFT regime.

Before drafting these Guidelines, the EBA carried out an impact assessment to establish whether to amend or repeal Guidelines JC/GL/2017/16 to fulfil the different mandates. At the same time, the EBA issued a Call for Input[2] to identify practical issues that financial institutions experience when complying with provisions in Regulation (EU) 2015/847 and Guidelines JC/GL/2017/16. It also had regard to emerging best practice set out by the FATF in its *2021 Updated Guidance for a Risk-Based Approach for Virtual Assets and Virtual Asset Service Providers*[3].

Based on this impact assessment, the responses to the EBA's Call for Input and the EBA's review of relevant FATF Guidance, the EBA concluded that most of the provisions and the overall risk-based approach set out in Guidelines JC/GL/2017/16 continue to be relevant and should be maintained, and that some provisions would benefit from greater detail to clarify regulatory expectations. It also concluded that the scale of changes necessary to extend the Guidelines to CASPs and the transfer of crypto-assets meant that Guidelines JC/GL/2017/16 should be repealed and replaced with new Guidelines.

New Guidelines

This section explains the rationale for provisions in the Guidelines that are new because they were not previously included in Guidelines JC/GL/2017/16.

A. Guidelines 2.1. on determining whether a card, instrument or device is used exclusively to pay for goods or services as per Article 2(3), point (a), and (5), point (b), of Regulation (EU) 2023/1113

Regulation (EU) 2023/1113 does not apply to the transfer of funds or transfer of electronic money tokens carried out using a payment card, an electronic money instrument, a mobile phone or any other digital or IT prepaid or postpaid device with similar characteristics used exclusively to pay for goods or services. Determining whether a card, instrument or device is used exclusively for this purpose can be difficult and may lead to divergent approaches. For this reason, the Guidelines set

2 https://www.eba.europa.eu/sites/default/documents/files/document_library/Publications/Other%20publications/2022/Call%20for%20input%20RTF/1041846/Call%20for%20Input.pdf

3 FATF (2021), 'Updated Guidance for a Risk-Based Approach to Virtual Assets and Virtual Asset Service Providers', https://www.fatf-gafi.org/en/publications/Fatfrecommendations/Guidance-rba-virtual-assets-2021.html

out common criteria for PSPs and CASPs on how to determine whether exclusions or derogations provided in Article 2(3), point (a), and (5), point (b), of Regulation (EU) 2023/1113 are met.

B. Guidelines 3. on steps to address technical limitations

Technical limitations refer to data-related constraints, boundaries or shortcomings that arise from the technological components, systems and frameworks involved in the processing of transfers. Examples of such limitations include limits to the amount, length and format of information that can be included in the transfer. Technical limitations can hamper the transfer of information as further specified in these Guidelines to ensure compliance with Regulation (EU) 2023/1113.

To address this, the Guidelines set out common criteria on the information PSPs and CASPs should include in relevant fields when transferring crypto-assets and funds in order to comply with Regulation (EU) 2023/1113. They also set out the steps CASPs and ICASPs should take if the full information cannot be transmitted due to technical limitations.

The Guidelines allow for a transitional period up to 31 July 2025 for CASPs and ICASPs, while systems are being adjusted to comply with the specifications to Regulation (EU) 2023/1113 as introduced by the Guidelines. The same transitional period is not foreseen for PSPs as the requirements that apply to them in Regulation (EU) 2023/1113 are similar to those in Regulation (EU) 2015/847.

C. Guidelines 3.1. on the interoperability of messaging or payment and settlement systems

For transfers of crypto-assets, several messaging or payment and settlement systems exist that address information transfer requirements, including open-network systems, closed-network systems and protocol-agnostic systems. Not all are interoperable, which means that CASPs might have to use multiple systems to be able to transact with their counterparties. This can create data integration issues and hamper institutions' ability to comply with travel rule requirements.

The Guidelines highlight that a system's architectures should be sufficiently robust to enable the transmission of information in a seamless and interoperable manner so that CASPs involved in the transfer chain can comply with the travel rule requirements.

D. Guidelines 4. on identifying the specific data points to be transmitted as part of the information required under Article 4(1) and (2) and Article 14(1) and (2) of Regulation (EU) 2023/1113

Regulation (EU) 2023/1113 specifies which information should be transmitted but does not set it out in detail, giving rise to divergent interpretations across different PSPs and CASPs including the risk that transfers with complete information could also be unnecessarily rejected.

To address this, the Guidelines set out common standards on information that PSPs and CASPs should include in the name, address and LEI / alternative identifier fields for crypto-assets and funds transfer purposes.

E. Guidelines 8. on self-hosted wallets

Regulation (EU) 2023/1113 requires CASPs to:

a) obtain and hold the information on the self-hosted address;

b) ensure that the transfer of crypto-assets can be individually identified; and

c) assess whether that address is owned or controlled by the CASP customer where the transfer amount exceeds EUR 1 000.

To address the practical challenges arising from the application of these requirements, the Guidelines provide details on the steps to be taken, with respect to self-hosted addresses, to:

a) individually identify a transfer;

b) identify a transfer from or to self-hosted addresses;

c) identify the originator and beneficiary;

d) prove the ownership or controllership (when applicable); and

e) put in place mitigating measures, where applicable.

F. Guidelines 9. on obligations on the payer's PSP, payee's PSP and IPSPs where a transfer is a direct debit

Direct debits are payment instructions sent by the PSP of the payee to the payer's PSP. Unlike a credit transfer, which is initiated by the payer, a direct debit is a transaction initiated by the payee. This means that the payee's PSP holds the information that the payer's PSP would need to comply with its obligations. As a result, in the direct debit context, the payer's PSP may not be able to comply with the requirements of Regulation (EU) 2023/1113 if it does not have the required information. These Guidelines set out what direct debit providers should do to comply with their legal obligations under Regulation (EU) 2023/1113.

Interaction with other guidelines

The Guidelines complement the following EBA guidelines:

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

[4] EBA/GL/2021/02.

- EBA Guidelines on policies and procedures in relation to compliance management and the role and responsibilities of the AML/CFT Compliance Officer under Article 8 and Chapter VI of Directive (EU) 2015/849[5];

- EBA Guidelines on outsourcing arrangements[6];

- EBA Guidelines on ICT and security risk management[7];

- EBA DRAFT Guidelines on internal policies, procedures and controls to ensure the implementation of Union and national restrictive measures[8];

- EBA DRAFT Guidelines on internal policies, procedures and controls to ensure the implementation of Union and national restrictive measures under Regulation (EU) 2023/1113 [9]; and

- ESMA DRAFT technical standards and guidelines specifying certain requirements of the Markets in Crypto-Assets Regulation (MiCAR) on detection and prevention of market abuse, investor protection and operational resilience[10].

[5] EBA/GL/2022/05.

[6] EBA/GL/2019/02.

[7] EBA/GL/2019/04.

[8] Guidelines under development available at https://www.eba.europa.eu/activities/single-rulebook/regulatory-activities/anti-money-laundering-and-countering-financing-0

[9] Guidelines under development available at https://www.eba.europa.eu/activities/single-rulebook/regulatory-activities/anti-money-laundering-and-countering-financing-0

[10] Guidelines under development available at https://www.esma.europa.eu/sites/default/files/2024-03/ESMA75-453128700-1002_MiCA_Consultation_Paper_-_RTS_market_abuse_and_GLs_on_investor_protection_and_operational_resilience.pdf

3. Guidelines on information requirements in relation to transfers of funds and certain crypto-assets transfers under Regulation (EU) 2023/1113 ('Travel Rule Guidelines')

EBA/GL/2024/11

4 July 2024

Guidelines

on information requirements in relation to transfers of funds and certain crypto-assets transfers under Regulation (EU) 2023/1113 ('Travel Rule Guidelines')

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

Reporting requirements

3. According to Article 16(3) of Regulation (EU) No 1093/2010, competent authorities must notify the EBA 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/2024/11'. Notifications should be submitted by persons with appropriate authority to report compliance on behalf of their competent authorities. Any change in the status of compliance must also be reported to the EBA.

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

[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

Subject matter and scope of application

5. These Guidelines fulfil the mandate to issue guidelines in accordance with Article 36, first and second subparagraphs, of Regulation (EU) 2023/1113[2].

6. Specifically, these Guidelines:

   a) set out the factors that payment service providers (PSPs), intermediary payment service providers (IPSPs), crypto-asset service providers (CASPs) and intermediary crypto-asset service providers (ICASPs) should consider when establishing procedures to detect and manage transfers of funds and crypto-assets lacking the required information on the payer/originator and/or the payee/beneficiary, and to ensure that these procedures are effective;

   b) specify what PSPs, CASPs, IPSPs and ICASPs should do to manage the risk of money laundering (ML) or terrorist financing (TF) where the required information on the payer, originator, payee or beneficiary is missing or incomplete;

   c) specify technical aspects of the application of Regulation (EU) 2023/1113 to direct debits.

7. In addition, these Guidelines fulfil the mandate to issue guidelines in accordance with Article 19a(2) of Directive (EU) 2015/849[3] specifying measures in relation to the identification and assessment of the risks of money laundering and terrorist financing associated with the transfer of crypto-assets directed to or originating from a self-hosted address.

Addressees

8. These Guidelines are addressed to:

   a) PSPs as defined in Article 3, point (5), of Regulation (EU) 2023/1113, and IPSPs as defined in Article 3, point (6), of Regulation (EU) 2023/1113;

   b) CASPs as defined in Article 3, point (15), of Regulation (EU) 2023/1113, and ICASPs as defined in Article 3, point (16), of Regulation (EU) 2023/1113;

[2] 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 (OJ L150, 9.6.2023, p. 1).

[3] Directive (EU) 2015/849 of the European Parliament and of the Council of 20 May 2015 on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing, amending Regulation (EU) No 648/2012 of the European Parliament and of the Council, and repealing Directive 2005/60/EC of the European Parliament and of the Council and Commission Directive 2006/70/EC (OJ L 141, 5.6.2015, p. 73).

c) competent authorities responsible for supervising PSPs, IPSPs, CASPs and ICASPs for compliance with their obligations under Regulation (EU) 2023/1113.

Definitions

9. Unless otherwise specified, terms used and defined in Regulation (EU) 2023/1113, in Directive (EU) 2015/849 and in Directive (EU) 2015/2366 have the same meaning in the Guidelines. Furthermore, for the purpose of these Guidelines, the following definitions apply:

Risk	Means the impact and likelihood of ML/TF taking place.
Risk factors	Means variables that, either on their own or in combination, may increase or decrease the ML/TF risk posed by an individual business relationship, occasional transaction or transfer.
Risk-based approach	Means an approach whereby competent authorities, PSPs, IPSPs, CASPs and ICASPs identify, assess and understand the ML/TF risks to which PSPs, IPSPs, CASPs and ICASPs are exposed and take AML/CFT measures that are proportionate to those risks.
Transfer chain	Means the end-to-end sequence of parties, processes and interactions involved in facilitating the transfer of funds and transfer of crypto-assets, as defined in Regulation (EU) 2023/1113, from the payer or originator to the payee or beneficiary.

3. Implementation

Date of application

10. These Guidelines apply from 30 December 2024.

Repeal

11. The 'Joint Guidelines under Article 25 of Regulation (EU) 2015/847 on the measures payment service providers should take to detect missing or incomplete information on the payer or the payee, and the procedures they should put in place to manage a transfer of funds lacking the required information'[4] are repealed with effect from 30 December 2024.

[4] JC/GL/2017/16.

4. Information requirements in relation to transfers of funds and certain crypto-asset transfers under Regulation (EU) 2023/1113

4.1. General provisions

Transfer of funds and crypto-assets

12. To determine what information should accompany a transfer of funds or crypto-assets, and the steps they should take to comply with Regulation (EU) 2023/1113, PSPs, IPSPs, CASPs and ICASPs should set out in their policies and procedures how they will establish for each transfer of funds or crypto-assets whether they act as:

    a) the PSP of the payer, the payee or an IPSP;

    b) the CASP of the originator, the beneficiary, or as an ICASP.

13. PSPs, IPSPs, CASPs and ICASPs should ensure that the policies and procedures they have put in place to comply with Articles 7(1 and 2), 8(1), 11(1 and 2), 12(1), 16(1), 17(1), 20 and 21(1) of Regulation (EU) 2023/1113 are effective and remain effective, for example by testing a random sample from all processed transfers.

14. PSPs, IPSPs, CASPs and ICASPs should keep their policies and procedures up to date and improve them as necessary.

4.2. Exclusion from the scope of Regulation (EU) 2023/1113 and derogations

Transfer of funds and crypto-assets

15. PSPs and CASPs should set out in their policies and procedures how they will determine whether the conditions for the application of the exclusions or derogations set out in Article 2 of Regulation (EU) 2023/1113 are met. PSPs and CASPs that are unable to establish that those conditions are met should comply with Regulation (EU) 2023/1113 in respect of all transfers of funds and crypto-assets.

4.2.1. Determining whether a card, instrument or device is used exclusively to pay for goods or services as referred to in Article 2(3), point (a), and (5), point (b), of Regulation (EU) 2023/1113

Transfer of funds and crypto-assets

16. PSPs and CASPs should treat a transfer of funds or crypto-assets as a payment for goods or services when the transfer is made from a customer (buyer) to a merchant (seller) in exchange for the purchase of goods or for the provision of services. To determine whether a card, instrument or device is used exclusively to pay for goods or services, PSPs and CASPs should establish that at least one of the following conditions is met:

    a) whether the functionality of the card, instrument or device used is restricted to pay for goods or services;

    b) whether a merchant categorisation code is assigned to customers, including payment card schemes' Merchant Category Code (MCC), that is used to categorise the type of goods or services sold;

    c) whether the customer is engaged in economic or professional activity, irrespective of its legal form, using information collected for the purposes of Article 13 of Directive (EU) 2015/849, if available, or information accessible via third-party providers or in publicly available sources; and

    d) the PSP's or CASP's analysis of trends and behaviours, including transfer history and patterns, allows it to determine whether the payer and originator make payments for goods or services, or the payee and beneficiary receive payments for goods or services.

4.2.2. Linked transfers in relation to the EUR 1 000 threshold as referred to in Articles 2(5), point (c), 5(2), 6(2) and 7(3) of Regulation (EU) 2023/1113

Transfer of funds

17. PSPs should have policies and procedures in place to detect transfers that appear to be linked.

18. PSPs should treat transfers as linked that are:

    a) carried out in a single operation or in several transactions; and

    b) sent by the same payer to the same payee, within a short timeframe; or

    c) sent from one payer to different payees or from different payers to the same payee within a short timeframe; including cases where different accounts are used belonging to the same person or different transactions are made intended for the same person, where that information is known by the PSP.

19. PSPs should set out in their policies and procedures:

    a) what constitutes a short timeframe for different types of transfers; PSPs should determine this timeframe in a way that is commensurate with the ML/TF risk to which their business is exposed, based on the risk assessments they have carried out in line with the EBA's ML/TF Risk Factors Guidelines[5];

[5] EBA/CP/2023/11.

b) how they will identify attempts to circumvent the threshold or evade detection; and

c) any other scenarios that might also give rise to linked transactions.

20. PSPs should determine whether a transfer is linked the moment the transfer was ordered or initiated, taking into account its absolute values, regardless of any charges levied by the PSP.

4.3. Transmitting and receiving information with the transfer in accordance with Articles 4 to 8, 10 to 12, 14 to 17 and 19 to 21 of Regulation (EU) 2023/1113

4.3.1. Messaging or payment and settlement systems

Transfer of funds and crypto-assets

21. PSPs, IPSPs, CASPs and ICASPs should use infrastructures and services for the transmission and reception of information that are technically capable of the full transmission and reception of information without gaps or errors in the presentation of the information as specified in these Guidelines.

22. PSPs, IPSPs, CASPs and ICASPs should ensure that their systems are able to maintain data integrity, in particular where information has to be converted into a different format before transmitting it or after receiving it. PSPs, IPSPs, CASPs and ICASPs that cannot ensure that their systems are able to transmit, receive or convert the information without error or omission should change to a system which is capable of that.

23. PSPs, IPSPs, CASPs and ICASPs should ensure that the systems they use for the transfer of information are secure. CASPs should also apply the guidance provided to PSPs by the EBA Guidelines on ICT and security risk management[6] and the EBA Guidelines on outsourcing arrangements[7].

Transfer of crypto-assets

24. CASPs and ICASPs may, by way of derogation from paragraph 21 and until 31 July 2025, exceptionally use infrastructures or services where technical limitations in relation to the completeness of data need to be compensated by additional technical steps or fixes to fully comply with these Guidelines. Those additional procedures should at least include alternative mechanisms for collecting, holding and making available to the receiving CASP or ICASP in the transfer chain the information that cannot be transmitted due to technical limitations.

25. When transmitting information in accordance with Article 14 of Regulation (EU) 2023/1113, the originator's CASP and ICASP should:

[6] EBA/GL/2019/04.

[7] EBA/GL/2019/02.

a) transmit the information either as part of, or incorporated into, the transfer on the blockchain or on another distributed ledger technology (DLT) platform, or independently via different communication channels – including via direct communication between CASPs, application programming interfaces (APIs), code solution running on top of the blockchain and other third-party solutions; and

b) transmit the required information immediately and securely and no later than the initiation of the blockchain transaction.

26. When choosing the messaging or payment and settlement system(s), CASPs and ICASPs should take proportionate, risk-sensitive measures to assess:

a) the system's ability to communicate with other internal core systems and with the messaging or payment and settlement systems of the counterparty of a transfer, and its compatibility with other blockchain networks;

b) the reachability of the protocol (i.e. the diversity and accuracy of counterparties that can be reached using the protocol – subject to the CASP's own due diligence assessment – and the rate of transfers that would successfully be sent to the intended beneficiary or received from the originator);

c) how the system enables the CASP or ICASP to detect a transfer with missing or incomplete information;

d) data integration capabilities, data security and data reliability of the system.

4.3.2. Multi-intermediation and cross-border transfers

Transfer of funds

27. PSPs and IPSPs that enable the execution of transfers with two or more IPSPs or PSPs on a cross-border basis should describe in their policies and procedures how the information on the payer and payee is transmitted throughout the transfer chain to the next PSP and IPSP in the transfer chain.

28. For transfers that have not been batched, the PSP or IPSP should:

a) consider the transfer chain (from end to end) as one such that the flow of information on the original payer and payee is preserved;

b) where the transfer is made from a cross-border channel to a domestic channel, select the domestic system that maximises the transparency of the cross-border nature of the transfer and ensures that the information about the parties transmitted to the next PSP in the payment chain can be readily understood by all intermediary and/or beneficiary PSPs;

c) in cases of doubt, assume that the transfer is a cross-border transfer, resulting in the use of appropriate payment channels that may facilitate the necessary transmission of information.

29. IPSPs are only responsible for passing through the payment message using the data that they have been provided with by the previous PSP/IPSP in the transfer chain, subject to the specific check required by Articles 10 to 13 of Regulation (EU) 2023/1113.

30. PSPs and IPSPs should not treat a transfer from the payer to the payee as liquidity movement or settlement on the PSP's and IPSP's own account.

Transfer of funds and crypto-assets

31. Where the intermediary does not receive the required information related to a transfer, particularly in the case of batch transfers, the IPSP or ICASP should obtain the missing information via an alternative channel mechanism, including methods such as APIs and third-party solutions, to comply with the requirements set in Regulation (EU) 2023/1113.

4.4. Information to be transmitted with the transfer in accordance with Articles 4 and 14 of Regulation (EU) 2023/1113

Transfer of funds and crypto-assets

32. PSPs and CASPs should not change the initial submission, unless:

    a) they are requested to do so by the IPSP, payee's PSP, ICASP or beneficiary's CASP, if the IPSP, payee PSP, ICASP or beneficiary CASP considers that some of the information under Articles 7, 11, 19 or 20 of Regulation (EU) 2023/1113 is missing; or

    b) following the transfer, the payer's PSP or originator's CASP detects an error in the information they transmitted to comply with Articles 4 and 14 of Regulation (EU) 2023/1113.

33. Where, in the context of paragraph 32, there is a change to the initial submission, the payer's PSP or originator's CASP should inform the next PSP and CASP in the transfer chain and submit the correct information. The next PSP and CASP in the transfer chain should then perform, once again, the necessary tasks to detect the missing or incomplete information.

4.4.1. Providing the payment account number of the payer in accordance with Article 4(1), point (b), of Regulation (EU) 2023/1113, and of the payee (Article 4(2), point (b), of Regulation (EU) 2023/1113)

Transfer of funds

34. PSPs should ensure that the transfer of funds is accompanied by the payment account number. Where the transfer of funds is made using a payment card, the number of that card (the Primary Account Number (PAN)) can take the place of the payment account number, on condition that that number allows the funds transfer to be traced back to the payer or the payee.

4.4.2. Providing the name of the payer, the payee, the originator and the beneficiary respectively in accordance with Articles 4(1), point (a), 4(2), point (a), 14(1), point (a), and 14(2), point (a), of Regulation (EU) 2023/1113

Transfer of funds and crypto-assets

35. The payer's PSP or originator's CASP should provide the following:

a) For natural persons, the full names and surnames of the customer as they appear in the customer's identity document, or in the electronic identification that complies with the standards in Article 13 of Directive (EU) 2015/849, or, if either is unavailable for a legitimate reason, documentation in accordance with the EBA Guidelines on policies and controls for the effective management of money laundering and terrorist financing (ML/TF) risks when providing access to financial services[8]. Where technical limitations exist as referred to in paragraph 24 that prevent the transmission of the customer's names and surnames, the originator's CASP should, as a minimum, include the first given name and last surname.

b) For legal persons, the name under which the legal person is registered. Where technical limitations exist as referred to in paragraph 24 that prevent the transmission of the full registered legal name, the originator's CASP should transmit the trading name. Trading names used should be able to be traced back unequivocally to the legal person and match any such names recorded in official registries.

c) For transfers from a joint account, address or wallet, the names of all holders of the account, address or wallet. Where technical limitations exist as referred to in paragraph 24 that prevent the transmission of all names of all parties to the transfer, the originator's CASP should transmit the name of the holder of the account, address or wallet that is initiating the transfer, or, where that is not possible, the primary account, address or wallet holder.

4.4.3. Providing the address of the payer and of the originator including the name of the country, official personal document number, and customer identification number or, alternatively, the date and place of birth of the payer in accordance with Articles 4(1), point (c), and 14(1), point (d), of Regulation (EU) 2023/1113

Transfer of funds and crypto-assets

36. The payer's PSP and originator's CASP should provide the following:

a) For natural persons, the usual place of residence of the payer or originator or, where there is no fixed residential address, the postal address at which the natural person can be reached. In the case of a vulnerable person, as referred to in paragraph 19(b) of the EBA Guidelines on policies and controls for the effective management of money laundering and terrorist financing (ML/TF) risks when providing access to financial services, who cannot reasonably be expected to provide an address in relation to their usual

[8] EBA/GL/2023/04.

place of residence, the PSP or the CASP may use an address that is provided in alternative documentation as referred to in paragraph 19(b) of the above Guidelines where such documentation contains an address and where its use is permitted under the national law of the payer.

b) For legal persons, the payer's or originator's registered or official office address.

37. The address should be provided, to the extent possible, in the following order of priority: the full country name or the abbreviation in accordance with the International Standard for country codes (ISO 3166) (alpha-2 or alpha-3), postal code, city, state and province and municipality, street name, building number or building name.

38. The payer's PSP and originator's CASP should provide the postal address as specified in paragraph 37. Without prejudice to paragraph 25(a), any alternatives to postal addresses, including post office box numbers and virtual addresses, should not be considered to meet the requirements under Article 4(1), point (c), and Article 14(1), point (d), of Regulation (EU) 2023/1113.

39. The combination of the alternative information items to be provided in accordance with Article 4(1), point (c), and 14(1), point (d), of Regulation (EU) 2023/1113 should not only be based on availability but also on the set of information which best provides for an unambiguous identification of the payer or originator.

40. For transfers from a joint account, address or wallet, the information of all holders of the account, address or wallet should be provided. Where the transmission of the respective information of all the parties cannot take place due to technical limitations as referred to in paragraph 24 the payer's PSP and originator's CASP should transmit the information of the holder of the account, address or wallet initiating the transfer, or, alternatively, of the primary account, address or wallet holder.

4.4.4. Providing an equivalent identifier to the LEI of the payer, the payee, the originator and the beneficiary in accordance with Articles 4(1), point (d), 4(2), point (c), 14(1), point (e), and 14(2), point (d), of Regulation (EU) 2023/1113

Transfer of funds and crypto-assets

41. The payer's PSP and the originator's CASP should consider only those official identifiers as equivalent to an LEI that:

a) are a single identification code that is unique to the legal entity;

b) are published in public registries;

c) are issued upon entity formation by a public authority in the jurisdiction in which the legal entity is based;

d) allow for the identification of the name and address elements; and

e) are accompanied by a description of the type of identifier used in the messaging system.

4.5. Detecting missing information in accordance with Articles 7, 11, 16 and 20 of Regulation (EU) 2023/1113

4.5.1. Procedures to detect missing information in accordance with Articles 7, 11, 16 and 20 of Regulation (EU) 2023/1113

Transfer of funds and crypto-assets

42. Procedures as referred to in Articles 7 11, 16 and 20 of Regulation (EU) 2023/1113 should at least contain the following:

a) the steps for the detection of missing, incomplete and meaningless information or inadmissible characters or inputs;

b) a combination of monitoring practices during and after the transfer commensurate with the level of ML/TF risk to which the transfers are exposed, determined in accordance with the EBA's ML/TF Risk Factors Guidelines; and

c) the criteria that help PSPs, IPSPs, CASPs and ICASPs identify risk-increasing factors, as described in paragraph 52.

4.5.2. Admissible characters or inputs checks on transfers of funds in accordance with Articles 7(1) and 11(1) of Regulation (EU) 2023/1113

Transfer of funds

43. Payees' PSPs and IPSPs should ensure that in relation to their messaging or payment and settlement systems:

a) they understand the system's validation rules;

b) the system contains all the fields necessary to obtain the information required in Regulation (EU) 2023/1113, as specified in Section 4.4.;

c) the system prevents the sending or receipt of transfers where inadmissible characters or inputs are detected; and

d) the system flags rejected transfers for manual review and processing.

44. Where a PSP's or IPSP's messaging or payment and settlement system does not meet all the criteria set out in paragraph 43, the PSP or IPSP should put in place controls to mitigate the shortcomings.

45. Payees' PSPs and IPSPs should set out in their policies and procedures:

a) how they will detect whether the fields relating to the information in the messaging or payment and settlement system have been filled with characters or inputs that comply with the conventions of that system; and

b) the steps they will take where the characters or inputs are not in line with the conventions of that system.

4.5.3. Monitoring of transfers in accordance with Articles 7(2), 11(2), 16(1) and 20 of Regulation (EU) 2023/1113

Transfer of funds and crypto-assets

46. Payees' PSPs, IPSPs, beneficiary's CASPs or ICASPs should set out in their policies and procedures how they will determine which transfers will be monitored during or after the transfer in accordance with Articles 7(2), 11(2), 16 (1) and 20 of Regulation (EU) 2023/1113. PSPs, IPSPs, CASPs and ICASPs should at least set out:

    a) which risk factors they will take into account in this assessment; and

    b) which risk-increasing factors, or combination of risk-increasing factors, will always trigger monitoring during the transfer, and which will trigger a targeted review after the transfer has taken place.

47. PSPs, IPSPs, CASPs and ICASPs should determine the risk factors based on those set out in the EBA's ML/TF Risk Factors Guidelines, as well as relevant risk factors from their business-wide risk assessment, and the sectoral or national risk assessment to the extent that this is available. The risk factors should at least include:

    a) transfers that exceed a predefined value threshold taking into account the average value of transfers they routinely process and what constitutes an unusually large transfer, based on their particular business model;

    b) transfers where the payer, originator, payee, beneficiary, payer's PSP, originator's CASP, payee's PSP or beneficiary's CASP are located in countries or territories that are subject to restrictive measures including targeted financial sanctions, or countries or territories that present a high risk of circumvention of restrictive measures or targeted financial sanctions;

    c) transfers where the payer, originator, payee, beneficiary, payer's PSP, originator's CASP, payee's PSP or beneficiary's CASP are based in a country associated with high ML/TF risk, including, but not limited to:

        i) countries identified as high risk by the European Commission in accordance with Article 9 of Directive (EU) 2015/849; and

        ii) countries which, on the basis of credible sources such as evaluations, mutual evaluations, assessment reports or published follow-up reports, have AML/CFT requirements that are not consistent with Directive (EU) 2015/849 or the FATF Recommendations and countries that have not effectively implemented those requirements;

d) transfers where the payer's PSP, originator's CASP, IPSP, ICASP, payee's PSP or beneficiary's CASP are located in a country that, based on publicly available information, has not yet implemented the obligation to obtain, hold and transmit information on the originator and beneficiary when conducting wire and virtual asset transfers;

e) transfers with entities based in a third country that does not have licensing regimes or does not regulate PSP activity in the case of funds transfers and CASP activities in the case of crypto-asset transfers;

f) transfers with self-hosted addresses;

g) transfers from or to accounts, addresses or wallets known to be linked with suspicious activity;

h) a negative AML/CFT compliance record of the prior PSP, IPSP, CASP or ICASP in the transfer chain, based on public information;

i) transfers from a PSP, IPSP, CASP or ICASP identified as repeatedly failing to provide required information without a justified reason, or from a PSP, IPSP, CASP or ICASP that has previously been known to fail to provide required information on a number of occasions without good reason, even if it did not repeatedly fail to do so;

j) use of other techniques to perform layering of transactions that hinders the tracing of crypto-assets by concealing the trail leading back to the originator, including, but not limited to:

   i) funds and crypto-assets received and rapidly transferred further, thus artificially extending the transfer chain;

   ii) anonymity-enhancing techniques, products or services, including, but not limited to, mixers or tumblers, Internet Protocol (IP) anonymisers and stealth addresses.

48. When considering whether or not a transfer raises suspicion, the PSPs, IPSPs, CASPs or ICASPs should take a holistic view of all ML/TF risk factors associated with the transfer and consider that missing or inadmissible information per se does not give rise to suspicion of ML/TF.

4.5.4. Missing information checks in accordance with Articles 7 (2), 11 (2), 16 (1) and 20 of Regulation (EU) 2023/1113

Transfer of funds and crypto-assets

49. The payee's PSP, beneficiary's CASP, IPSP and ICASP should treat information as missing if fields are left empty, or if the information provided is meaningless or incomplete.

50. The payee's PSP, beneficiary's CASP, IPSP and ICASP should treat at least the following information as meaningless:

   a) strings of random or illogical characters (such as 'xxxxx', or 'ABCDEFG');

b) use of titles (such as Dr or Mrs) without the person's name;

c) other designations that are incoherent or unintelligible (such as 'An Other', or 'My Customer').

51. Where PSPs, CASPs, IPSPs and ICASPs use a list of terms commonly found to be meaningless, they should periodically review this list to ensure it remains relevant.

4.6. Transfers with missing or incomplete information in accordance with Articles 8, 12, 17 and 21 of Regulation (EU) 2023/1113**Risk-based procedures for determining whether to execute, reject or suspend a transfer in accordance with Articles 8(1), 12, 17(1) and 21(1) of Regulation (EU) 2023/1113**

Transfer of funds and crypto-assets

52. PSPs and CASPs should set out in their policies and procedures how they will determine whether to reject, suspend or execute a transfer in accordance with Articles 8(1), 12, 17(1) and 21 of Regulation (EU) 2023/1113. As part of this, PSPs and CASPs should list the risk factors that they will consider for each transfer.

53. PSPs, IPSPs, CASPs, and ICASPs should consider in their assessment before deciding on the appropriate course of action whether or not:

a) the information allows for determination of the subjects of the transfer; and

b) one or more risk-increasing factors have been identified that may suggest that the transfer presents a high ML/TF risk or gives rise to suspicion of ML/TF.

4.6.2. Rejecting or returning a transfer in accordance with Articles 8(1), point (a), 12, point (a), 17(1), point (a), and 21(1), point (a), of Regulation (EU) 2023/1113

Transfer of funds and crypto-assets

54. Where an IPSP, payee's PSP, ICASP or beneficiary's CASP decides to reject a transfer or an ICASP or beneficiary's CASP decides to return a transfer instead of requesting the missing information, they should inform the prior PSP, IPSP, CASP or ICASP in the transfer chain that the transfer has been rejected or returned because of missing information.

Transfer of crypto-assets

55. Where the rejection is technically not possible, the transfer should be returned to the originator. Where returning the transfer to the original address is not possible, CASPs should apply alternative methods. The alternative methods should be set out in their policies, and should include holding the returned assets in a secure, segregated account while communicating with the originator to arrange a suitable return method to the originator.

4.6.3. Requesting required information in accordance with Articles 8(1), point (b), 12(1), point (b), 17(1), point (b), and 21 (1), point (b), of Regulation (EU) 2023/1113

Transfer of funds and crypto-assets

56. Where the PSP, IPSP, CASP or ICASP requests required information that is missing, it should set a reasonable deadline by which the information should be provided. This deadline should not exceed three working days for transfers taking place within the Union, and five working days for transfers received from outside of the Union, starting from the day the PSP, CASP, IPSP or ICASP identifies the missing information. Longer deadlines up to seven days may be set where transfer chains involve:

    a) more than two parties in the transfer flow, including intermediaries and non-banks;

    b) at least one PSP, IPSP, CASP or ICASP that is based outside of the EU.

57. Where a PSP, IPSP, CASP or ICASP decides to request the required information from the prior PSP, IPSP, CASP or ICASP in the transfer chain it should notify the prior PSP, IPSP, CASP or ICASP in the transfer chain of the technical actions taken on that transfer due to missing or incomplete information, as applicable.

58. Any request for information or clarification should be sent through the same messaging system that was used for transmitting the required information or, where technical limitations exist as referred to in paragraph 24, secure methods of contact in line with the provisions and obligations of Regulation (EU) 2016/679.

Transfer of funds

59. Should the requested information not be forthcoming, the PSP or IPSP should send a reminder to the prior PSP or IPSP in the transfer chain and advise the prior PSP or IPSP in the transfer chain of the actions it may take should the PSP or IPSP fail to provide the requested information by the set deadline.

60. Where the requested information is not provided by the set deadline, the PSP or IPSP should make the decision on whether to reject, suspend or execute the transfer in line with its risk-based policies and procedures as specified in paragraphs 41 and 42. In addition to that decision it should, irrespective of whether the failure was repeated or not, consider the future treatment of the prior PSP or IPSP in the transfer chain for AML/CFT compliance purposes, including rejecting any future transfers from or to the prior PSP or IPSP in the transfer chain, or restricting or terminating its business relationship with that PSP or IPSP.

Transfer of crypto-assets

61. Should the requested information not be forthcoming, as part of actions to be taken in accordance with Articles 17 and 21 of Regulation (EU) 2023/1113, CASPs or ICASPs should consider sending a reminder to the prior CASP or ICASP in the transfer chain and advise the prior CASP

or ICASP in the transfer chain of the actions they may take should the CASP or ICASP fail to provide the required information before the set deadline.

62. Where the requested information is not provided by the set deadline, the CASP or ICASP should make the decision on whether to reject, return, suspend or execute the transfer in line with its risk-based policies and procedures as specified in paragraphs 52 and 53. In addition to that decision it should, irrespective of whether the failure was repeated or not, consider the future treatment of the prior CASP or ICASP in the transfer chain for AML/CFT compliance purposes, including rejecting any future transfers from or to the prior CASP or ICASP or self-hosted address in the transfer chain, or restricting or terminating its business relationship with it.

63. Requests for missing information or clarification with respect to transfers from or to self-hosted addresses should be sent directly to the CASP's customer.

4.6.4. Executing a transfer in accordance with Articles 8(1), 12(1), 17(1) and 21(1) of Regulation (EU) 2023/1113

Transfer of funds and crypto-assets

64. Where a PSP, IPSP, CASP or ICASP becomes aware that required information is missing, incomplete or provided using inadmissible characters during the transfer and executes the transfer, it should document the reason for executing that transfer and, in line with its risk-based policies and procedures, consider the future treatment of the prior PSP, IPSP, CASP, ICASP or self-hosted address in the transfer chain for AML/ CFT compliance purposes. However, where the payer, payee, originator or beneficiary cannot be unambiguously identified due to missing or incomplete information, or information provided using inadmissible characters, the PSP, IPSP, CASP or ICASP should not execute the transfer.

4.6.5. Detecting missing or incomplete information after executing a transfer in accordance with Articles 8(1), 12(1), 17(1) and 21(1) of Regulation (EU) 2023/1113

Transfer of funds

65. Where a PSP or IPSP detects ex post that the required information was missing, incomplete or provided using inadmissible characters, it should ask the prior PSP or IPSP in the transfer chain to provide the missing information, or to provide that information using admissible characters or inputs, applying Section 4.6.3.

Transfer of crypto-assets

66. Where a CASP or ICASP executes the transfer and detects ex post that the required information is missing or incomplete, it should ask the prior CASP or ICASP in the transfer chain to provide the missing information, in line with Section 4.6.3.

4.7. Repeatedly failing PSPs, CASPs, IPSPs or ICASPs in accordance with Articles 8 (2), 12 (2), 17 (2) and 21(2) of Regulation (EU) 2023/1113

4.7.1. Treatment of repeatedly failing PSPs, CASPs, IPSPs or ICASPs in accordance with Articles 8(2), 12(2), 17(2) and 21(2) of Regulation (EU) 2023/1113

Transfer of funds and crypto-assets

67. PSPs and CASPs should set out in their policies and procedures the quantitative and qualitative criteria they will use to determine whether a PSP, IPSP, CASP or ICASP is 'repeatedly failing' and document all transfers with missing or incomplete information.

68. Quantitative criteria should include at least:

    a) the percentage of transfers with missing or incomplete information sent by a specific PSP, IPSP, CASP or ICASP within a specific timeframe; and

    b) the percentage of follow-up requests that were left unanswered or were not adequately answered by a certain deadline.

69. Qualitative criteria should include at least:

    a) the level of cooperation of the requested PSP, IPSP, CASP or ICASP relating to previous requests for missing information;

    b) the existence of an agreement with the PSP, IPSP, CASP or ICASP requiring more time to provide the information;

    c) the type of information missing or incomplete and the reason given by the PSP, IPSP, CASP or ICASP for not providing the information.

70. The warning in accordance with Articles 8(2), point (a), 12(2), point (a), 17(2), point (a), and 21(2), point (a), of Regulation (EU) 2023/1113 should inform the prior PSP, IPSP, CASP or ICASP in the transfer chain of the steps that will be applied, should it continue to fail to provide the required information, including deadlines.

71. PSPs and CASPs should consider issuing a further warning to the prior PSP, IPSP, CASP or ICASP in the transfer chain that any future transfers will be rejected.

72. In relation to the treatment under Articles 8(2), point (b), 12(2), point (b), 17(2), point (b), and 21(2), point (b), of Regulation (EU) 2023/1113, PSPs and CASPs should consider how the repeated failure by the prior PSP, IPSP, CASP or ICASP in the transfer chain to provide information and that PSP's and CASP's attitude to responding to such requests affect the ML/TF risk associated with that PSP or CASP, and, where appropriate, carrying out real-time monitoring of all transactions received from them.

73. Before taking the decision to terminate a business relationship, in particular where the prior PSP, IPSP, CASP or ICASP in the transfer chain is a respondent counterparty from a third country, PSPs, IPSPs, CASPs and ICASPs should consider whether or not the risk can be managed in other ways, including ex ante through the application of enhanced due diligence measures in line with Article 19 of Directive (EU) 2015/849.

4.7.2. Reporting repeatedly failing PSPs, CASPs, IPSPs or ICASPs to the competent authority in accordance with Articles 8(2), 12(2), 17(2) and 21(2) of Regulation (EU) 2023/1113

Transfer of funds and crypto-assets

74. The report to the competent authority referred to in Articles 8(2), 12(2), 17(2) and 21 of Regulation (EU) 2023/1113 should be submitted by the PSPs, IPSPs, CASPs and ICASPs without undue delay, and no later than three months after identifying the repeatedly failing PSP, IPSP, CASP or ICASP. Reporting should take place regardless of the reasons given by the 'repeatedly failing' PSP, IPSP, CASP or ICASP, if any, to justify that breach, or their location in the Union or outside.

75. The report should include:

    a) the name of the PSP, IPSP, CASP or ICASP identified as repeatedly failing to provide the required information;

    b) the country in which the PSP, IPSP, CASP or ICASP is authorised;

    c) the nature of the breach, including:

        i. the frequency of transfers with missing information;

        ii. the period of time during which the breaches were identified; and

        iii. any reasons the PSP, IPSP, CASP or ICASP may have given to justify their repeated failure to provide the required information;

    d) details of the steps the reporting PSP, IPSP, CASP or ICASP took.

4.8. Transfers of crypto-assets made from or to self-hosted addresses in accordance with Articles 14(5) and 16(2) of Regulation (EU) 2023/1113

4.8.1. Individually identifying transfers from or to self-hosted addresses in accordance with Articles 14(5) and 16(2) of Regulation (EU) 2023/1113

76. CASPs and ICASPs should consider a transfer of a crypto-asset as individually identified when:

a) a unique identifier for each transfer is used, such as a transfer hash or a reference number; or

b) additional information is included in the transfer to help identify the transfer.

4.8.2. Identification of a transfer from or to a self-hosted address

77. To determine whether or not a self-hosted address is used on the other end of a transfer, the originator's CASP and the beneficiary's CASP should rely on available technical means including but not limited to blockchain analytics, third-party data providers and identifiers used by messaging systems.

78. If such information cannot be retrieved via technical means, the originator's CASP and the beneficiary's CASP should obtain that information directly from its customer. Where, in this case, the originator's CASP and the beneficiary's CASP establish that the transfer is made to or from another CASP, the originator's CASP and the beneficiary's CASP should take the necessary steps to accurately identify the counterparty CASP.

79. The originator's CASP should do this assessment before the transfer is initiated and the information transmitted in accordance with Article 14(5) of Regulation (EU) 2023/1113; the beneficiary's CASP should do this assessment before the crypto-assets are made available to the beneficiary in accordance with Article 16(2) of that Regulation.

4.8.3. Identification of the originator and beneficiary in a transfer from or to a self-hosted address

80. Where a self-hosted address is used on the other end of the transfer, CASPs should collect the information on the originator or beneficiary from their customer.

4.8.4. Transfers above EUR 1 000 and proof of ownership or controllership of a self-hosted address

81. CASPs should determine whether a transfer involving a self-hosted address amounts to or exceeds EUR 1 000:

a) at the moment the transfer was ordered or initiated, in the case of the originator's CASP; or

b) at the time of the receipt, in the case of the beneficiary's CASP.

82. To determine whether the value of transfers from or to self-hosted addresses is above EUR 1 000, the CASPs should use the exchange rate of the crypto-asset being transferred to determine its value in euros at the time of the transfer, and regardless of any transaction fees.

83. In order to assess whether the self-hosted address is owned or controlled by the originator or beneficiary, respectively, CASPs should use at least one of the following verification methods:

a) unattended verifications as specified in the Guidelines on the use of Remote Customer Onboarding Solutions under Article 13(1) of Directive (EU) 2015/849[9] displaying the address;

b) attended verification as specified in the Guidelines on the use of Remote Customer Onboarding Solutions under Article 13(1) of Directive (EU) 2015/849;

c) sending of a predefined amount (preferably the smallest denomination of a given crypto-asset), set by the CASP, from and to the self-hosted address to the CASP's account;

d) requesting the customer to digitally sign a specific message into the account and wallet software with the key corresponding to that address;

e) other suitable technical means as long as they allow for reliable and secure assessment and the CASP is fully satisfied that it knows who owns or controls the address.

84. The decision on which method(s) to choose should depend on:

a) the technical capabilities of the self-hosted address;

b) the robustness of the assessment each method can deliver; and

c) the ML/TF risk.

85. Where one method on its own is not sufficiently reliable to reasonably ascertain the ownership or controllership of a self-hosted address, the CASP should use a combination of methods.

86. Where the CASP is fully satisfied that the self-hosted address is owned or controlled by its customer, the CASP should document this in its systems and may not need to re-apply the measures above to subsequent transactions from/to the same address ('whitelisting'). A CASP making use of whitelisting should have controls in place to identify changes in the ML/TF risk of the self-hosted address and its ownership or controllership. Should the CASP establish that the ML/TF risk of the self-hosted address has changed or that there are indications that its customer no longer owns or controls the self-hosted address, it should remove this address from its whitelist.

4.8.5. Mitigating measures to put in place regarding transfers from or to a self-hosted address

87. CASPs should assess the risk associated with transfers from or to a self-hosted address as set out in Section 4.5.3. and in accordance with the EBA's ML/TF Risk Factors Guidelines, using all information related to originators and beneficiaries, patterns and geographies, and information from regulators, law enforcement and third parties.

[9] EBA/GL/2022/15.

88. CASPs should apply at least one of the risk-mitigating measures as identified in Article 19a(1) of Directive (EU) 2015/849 that are commensurate with the risks identified including where the CASP:

    a) is or becomes aware that the information on the originator or beneficiary using the self-hosted address is inaccurate; or

    b) encounters unusual or suspicious patterns of transactions or situations of higher ML/TF risk associated with transfers involving self-hosted addresses, in accordance with the EBA's ML/TF Risk Factors Guidelines.

89. Where, as a result of the assessment in Section 4.8.4., it is established that the self-hosted address is owned or controlled by a third person instead of the CASP's customer, the verification referred to in Article 19a(1), point (a), of Directive (EU) 2015/849 can be deemed to have taken place if:

    a) the CASP collects additional data from other sources to verify the submitted information, including but not limited to blockchain analytical data, third-party data, recognised authorities' data and publicly available information, as long as these are reliable and independent.

    b) the CASP uses other suitable means as long as the CASP is fully satisfied that it knows the identity of the originator or beneficiary and can demonstrate this to its competent authority.

90. Where such transfers raise suspicions of ML/TF, CASPs should report to the FIU in accordance with Directive (EU) 2015/849.

4.5. Obligations on the payer's PSP, payee's PSP and IPSPs where a transfer is a direct debit

Transfer of funds

91. Where a transfer of funds is a direct debit, the payee's PSP should send the required information on the payer and on the payee to the payer's PSP as part of the direct debit collection. Upon receipt of this information by the payer's PSP, the payee's PSP and IPSP should consider the information requirements in Article 4, points (2) and (4), and Article 5, points (1) and (2), of Regulation (EU) 2023/1113 to be met.

92. For the purpose of paragraph 91:

    a) the obligations set out in Articles 4, 5 and 6 of Regulation (EU) 2023/1113 should be applied to the payee's PSP;

    b) verification in Article 4(4) of Regulation (EU) 2023/1113 should be carried out by the payee's PSP on the information of the payee, before sending the direct debit collection;

c) the obligations set out in Articles 7, 8 and 9 of Regulation (EU) 2023/1113 should be applied to the payer's PSP (debtor PSP);

d) verification in Article 7(3) and (4) of Regulation (EU) 2023/1113 should be carried out by the payer's PSP (debtor PSP) on the information of the payer before debiting the payer's account.

93. Where the payer's PSP becomes aware, when receiving the direct debit collections, that the information referred to in Articles 4, 5 and 6 of Regulation (EU) 2023/1113 is missing or incomplete or has not been filled in using characters or inputs admissible in accordance with the conventions of the messaging or payment and settlement system as referred to in Article 7(1) of that Regulation, the options set out in Article 8(1), second subparagraph, of that Regulation should be applied by the payer's PSP. The payer's PSP should choose to ask for the required information on the payer and the payee before or after debiting the payer's account, in a risk-based approach. In particular, it should assess whether the payment should still be credited where information is missing or whether funds should be made available to the payee relying on information obtained from the payer and verified as part of the customer's due diligence process, in accordance with Section 4.4.

94. The payer's PSP should leverage available communication channels to engage with any repeatedly failing payee's PSP prior to taking further actions to restrict or reject payments. Where PSPs rely on information obtained prior to the transactions, their policies and procedures should take into consideration possible changes to information across time, in particular including name and address.

4. Accompanying documents

4.1. Cost-benefit analysis / impact assessment

In 2017, the European Supervisory Authorities (ESAs) issued *Joint Guidelines under Article 25 of Regulation (EU) 2015/847 on the measures payment service providers should take to detect missing or incomplete information on the payer or the payee, and the procedures they should put in place to manage a transfer of funds lacking the required information* (hereinafter 'Joint Funds Transfer Guidelines'). Article 25 of Regulation (EU) 2015/847 required the ESAs to issue guidelines to competent authorities and payment service providers (PSPs) on the measures to be taken in accordance with that Regulation, in particular as regards the implementation of Articles 7, 8, 11 and 12.

More recently, the European Commission issued a legislative package in July 2021 with four proposals in the area of AML/CFT, including a proposal for a recast of Regulation (EU) 2015/847, expanding the traceability requirements to crypto-assets. This recast is now published in the Official Journal of the European Union as Regulation (EU) 2023/1113 and it has a series of mandates assigned to the European Banking Authority (EBA), namely to issue guidelines to competent authorities, PSPs and crypto-asset service providers (CASPs) on:

- the measures those providers should take to comply with Regulation (EU) 2023/1113 and in relation to the implementation of Articles 7, 8, 11 and 12, and Articles 14 to 17, and Articles 19 to 22 – as per the first paragraph of Article 36;
- the technical aspects of the application of this Regulation to direct debits – as per the second paragraph of Article 36; and
- the measures, including the criteria and means for identification and verification of the identity of the originator or beneficiary of a transfer made to or from a self-hosted address, in particular through reliance on third parties, taking into account the latest technological developments – as per the amendments to Article 19a(2) of Directive (EU) 2015/849 as introduced by Article 38.

In this context, the EBA repealed the Joint Funds Transfer Guidelines and developed this consultation paper on the measures PSPs and CASPs should take to detect missing or incomplete information on the payer/originator or the payee/beneficiary, and the procedures they should put in place to manage a transfer of funds or crypto-assets lacking the required information, under Regulation (EU) 2023/1113 (Travel Rule Guidelines).

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 document provides an overview of the issues identified, the options considered and the potential impact of these options on PSPs, CASPs and competent authorities. As the Joint Funds Transfer Guidelines are repealed, this IA is performed on

the entire Travel Rule Guidelines and not just on the modifications resulting from Regulation (EU) 2023/1113[10]. The IA is high level and qualitative in nature.

A. Problem identification and background

Tracking financial flows can be an important tool in the prevention, detection and investigation of terrorist financing and other financial crimes.[11] This is also important for crypto-asset transfers, given that these are also subject to similar money laundering and terrorist financing (ML/TF) risks to fund transfers. This was taken into consideration in the EU's 2020 *Action plan for a comprehensive Union policy on preventing ML/TF*[12] and in Regulation (EU) 2023/1113, which was adopted to safeguard the full traceability of the transfer of funds and crypto-assets, ensuring the transmission of information on the payer, originator, payee and beneficiary throughout the transfer chain. This Regulation also requires PSPs and CASPs to put in place effective systems and controls to detect transfers that lack the required information, and risk-based policies and procedures to determine whether to execute, reject or suspend a transfer that lacks the required information. However, Regulation (EU) 2023/1113 does not set out in detail what PSPs and CASPs must do to comply. There is, therefore, a possibility that PSPs, CASPs and competent authorities may interpret and apply these regulations inconsistently, leaving the Union's financial market exposed to the risk of ML/TF.

B. Policy objectives

Through the Travel Rule Guidelines, the EBA aims to promote the development of a common understanding, by PSPs, CASPs and competent authorities across the EU, of effective procedures to detect and manage transfers of funds and crypto-assets that lack the information on the payer, originator, payee or beneficiary required by Regulation (EU) 2023/1113. A common understanding is essential to ensure the consistent interpretation and application of Union law and will be conducive to a stronger European anti-money laundering and countering the financing of terrorism (AML/CFT) regime.

As part of this, the Travel Rule Guidelines should not only set clear regulatory and supervisory expectations, but at the same time leave sufficient room for PSPs and CASPs to define their approach in a way that is proportionate to the nature and size of their business and commensurate with the ML/TF risk to which they are exposed.

[10] As such, some costs/benefits related to PSPs and competent authorities (in the context of their PSP supervision) described in the present IA might have been already incurred by them.

[11] European Commission (2016), 'Action plan to strengthen the fight against terrorist financing', February 2016.

[12] https://finance.ec.europa.eu/publications/action-plan-comprehensive-union-policy-preventing-money-laundering-and-terrorism-financing_en

C. Baseline scenario

In October 2008, the ESAs' predecessors published a *Common understanding of the obligations imposed by European Regulation 1781/2006 on the information on the payer accompanying fund transfers to payment service providers of payees*[13]. This common understanding determines how PSPs and competent authorities interpret their obligations under Regulation (EC) 1781/2006, which preceded Regulation (EU) 2015/847 and Regulation (EU) 2023/1113. While many of the common understanding's conclusions remain important, the scope and underlying legal basis have changed to reflect revised international standards and best practices. Furthermore, the common understanding did not compel financial institutions and competent authorities to 'comply or explain'. To address that, in 2017 the ESA's published the Joint Funds Transfer Guidelines, as mandated by Regulation (EU) 2015/847[14]. However, these Guidelines did not include CASPs and related competent authorities either, because they were outside of the scope of the EU's AML/CFT regime.

In the baseline scenario, the implementation of Regulation (EU) 2023/1113 takes effect without accompanying EBA guidelines, but with a non-binding common understanding that addresses some, but not all, aspects of Regulation (EU) 2023/1113.

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

Section D presents the main policy options discussed and the decisions made by the EBA during the development of the Travel Rule 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.

In drafting these Guidelines, with regard to the points relating to the transfer of funds the EBA did not aim to change the substance of requirements set by the Joint Funds Transfer Guidelines which derive from the views gathered back in 2017 from PSPs and related competent authorities, but enhanced the points escalated to the EBA staff during the Call for Input exercise[15]. Specifically with regard to crypto-assets, the EBA considered the views of AML/CFT competent authorities and informal technical input from private sector stakeholders. Different options on the scope of the mandate and the approach of the Guidelines have been identified, and their costs and benefits assessed for their ability to achieve the EBA's policy objectives.

[13] https://www.eba.europa.eu/sites/default/documents/files/documents/10180/16166/3223f568-011c-4781-9a48-c0f68fda298c/2008%2016%2010%20AMLTF%20Common%20understanding%20on%20payment%20funds%20transfer.pdf?retry=1

[14] As mentioned previously, as the Joint Funds Transfer Guidelines are repealed, this IA is done on the entire Travel Rule Guidelines and not just on the modifications due to the recast of Regulation (EU) 2015/847. Hence, as mentioned in the following paragraph, the baseline scenario described is the scenario before the Joint Funds Transfer Guidelines.

[15] https://www.eba.europa.eu/sites/default/documents/files/document_library/Publications/Other%20publications/2022/Call%20for%20input%20RTF/1041846/Call%20for%20Input.pdf

Scope of the mandate

Regulation (EU) 2023/1113 mandates the EBA to issue guidelines to competent authorities and PSPs/IPSPs and CASPs/ICASPs on:

- the measures the providers should take to comply with Regulation (EU) 2023/1113 and in relation to the implementation of Articles 7, 8, 11 and 12, and Articles 14 to 17, and Articles 19 to 22 – as per the first paragraph of Article 36;
- the technical aspects of the application of this Regulation to direct debits – as per the second paragraph of Article 36; and
- the measures, including the criteria and means for identification and verification of the identity of the originator or beneficiary of a transfer made to or from a self-hosted address, in particular through reliance on third parties, taking into account the latest technological developments – as per the amendments to Article 19a(2) of Directive (EU) 2015/849 as introduced by Article 38.

Option 1.1: The EBA could focus on the articles listed in the mandate and on other articles where this is necessary to ensure the consistent application of the Regulation's obligations.

Option 1.2: The EBA could write guidelines exclusively on the articles listed in the mandate.

Approach

Guidelines need to be targeted and proportionate, but the first and second paragraph of Article 36, and the amendments to Article 19a(2) of Directive (EU) 2015/849, as introduced by Article 38, do not prescribe the approach the EBA should take. While Regulation (EU) 2023/1113 forms part of the Union's wider AML/CFT framework, which is risk-based, the Regulation contains a number of provisions that are prescriptive and leave PSPs/IPSPs, CASPs/ICASPs and competent authorities little room for manoeuvre.

Option 2.1: The Guidelines could be detailed and prescriptive with a view to achieving maximum harmonisation of PSPs'/IPSPs' and CASPs'/ICASPs' approaches to complying with Regulation (EU) 2023/1113.

Option 2.2: The Guidelines could provide enough detail to enable PSPs/IPSPs and CASPs/ICASPs to identify areas of high risk and focus their efforts in complying with Regulation (EU) 2023/1113 on those areas, but leave it to PSPs/IPSPs and CASPs/ICASPs to decide how best to comply.

Option 2.3: The Guidelines could prescribe what PSPs/IPSPs and CASPs/ICASPs should do in certain situations, whilst allowing them some flexibility to accommodate different risk scenarios.

E. Cost-benefit analysis and preferred options

The implementation of the different options would create both benefits and costs for PSPs/IPSPs, CASPs/ICASPs and competent authorities. All options the EBA has considered create one-off costs for PSPs/IPSPs and CASPs/ICASPs to review and adapt existing systems and controls, and ongoing costs for PSPs/IPSPs, CASPs/ICASPs and competent authorities to train staff in the application and assessment of these systems and controls. However, these costs derive mainly from changes to the Union's legal framework. Moreover, with respect to the transfer of funds, the Travel Rule Guidelines allow PSPs/IPSPs to build on systems established under the 2017 Joint Funds Transfer Guidelines, which can limit the costs for some PSPs/IPSPs that already apply the principles set out in the Guidelines and for the supervision of these systems by competent authorities.

Scope

The main advantage of Option 1.1 would be that greater regulatory certainty would be achieved in key areas where this is necessary to achieve a consistent and effective pan-European approach. Examples of areas that would benefit from additional guidelines for PSPs/IPSPs and CASPs/ICASPs include the determination of the transfer of goods and services (Article 2(3), point (a), and (5), point (b), of Regulation (EU) 2013/1113) and determining whether a transfer between PSPs, their agents or branches made for their own account is not subject to Regulation (EU) 2023/1113 (Article 2(2)). Furthermore, to provide guidance on the assessment and reporting by PSPs, IPSPs, CASPs and ICASPs (Articles 9, 13, 18 and 22 of Regulation (EU) 2013/1113, respectively) would also create more consistency. In addition, giving guidance for payers' PSPs on the information accompanying the transfer of funds would mirror the guidance on the information accompanying the transfer of crypto-assets for originators' CASPs, as required by the mandate (Articles 4 to 6). The disadvantage of Option 1.1 is that, under this option, PSPs/IPSPs and CASPs/ICASPs could incur greater one-off costs for reviewing and updating their systems and controls in light of new expectations compared to the baseline scenario or Option 1.2. For PSPs/IPSPs, however, the main costs are largely absorbed by the costs associated with the modifications of the underlying ML/TF framework.

The main advantage of Option 1.2 is that guidelines that focus exclusively on the mandates listed in the first and second paragraph of Article 36, and the amendments to Article 19a(2) of Directive (EU) 2015/849, as introduced by Article 38, are conducive to achieving consistency where the legislature feels this is necessary with lower compliance costs. Option 1.2 is therefore likely to be more targeted than Option 1.1. However, certain provisions in Regulation 2023/1113 are not sufficiently clear or detailed, nor are they addressed in other supranational guidelines, so they could therefore be interpreted differently by competent authorities and PSPs/IPSPs and CASPs/ICASPs in different Member States, as demonstrated by the different exercises with the industry organised by the EBA.

Option 1.1 is the retained option. The benefits associated with greater regulatory certainty and consistency of approach that can be expected from guidelines on issues beyond those described in the first and second paragraph of Article 36 and the amendments to Article 19a(2) of Directive (EU) 2015/849, as introduced by Article 38, are expected to outweigh the additional compliance costs

(keeping in mind that these costs are largely absorbed by the costs associated with the modifications of the underlying ML/TF framework) for PSPs/IPSPs and CASPs/ICASPs. Option 1.1 reduces the risk of creating regulatory arbitrage and reduces compliance costs for PSPs/IPSPs and CASPs/ICASPs that operate across borders and whose approach may otherwise be deemed inadequate by another competent authority or EU counterparty. It also ensures a more harmonised European approach for providing the required information on the transfer of funds and crypto-assets which is tailored to the areas of highest need, and a more effective fight, in particular, against ML/TF.

Approach

The main advantage of Option 2.1 is that detailed and prescriptive guidelines would reduce uncertainty and create maximum harmonisation of practices. Some industry representatives, as a result of the Call for Input, suggested this might be desirable, for instance, for the transfer of funds. However, the initial set-up costs are likely to be high, as PSPs/IPSPs and CASPs/ICASPs would have to adjust their systems to match the enhanced guidance, and ongoing compliance costs might increase for PSPs/IPSPs and CASPs/ICASPs whose size or business models might be better suited for alternative systems and controls. Furthermore, due to the dynamic and fast-paced evolvement of PSPs' and CASPs' business models, the Travel Rule Guidelines would be at risk of becoming outdated in the near future due to the level of granularity they would have to cover. For competent authorities, Option 2.1 would facilitate the assessment of PSPs'/CASPs' systems and controls to comply with Regulation (EU) 2023/1113, as prescriptive guidelines could reduce the need for specialist supervisors to exercise informed judgement.

The advantage of Option 2.2 is that it would allow PSPs/IPSPs and CASPs/ICASPs to identify and focus on those areas where the risk of ML/TF associated with transfers of funds and crypto-assets is highest in their own set-up. This approach would allow PSPs/IPSPs and CASPs/ICASPs to adopt the approach that is best suited to their particular nature and size — for example, some PSPs which are not credit institutions and some CASPs have suggested that 'one size does not fit all'. However, Option 2.2 would not achieve the same degree of regulatory certainty as Option 2.1 and could create costs by distorting competition, as PSPs/IPSPs (which escalated this point in the Call for Input as well), CASPs/ICASPs and competent authorities in different Member States could interpret the same guidance differently. PSPs/IPSPs and CASPs/ICASPs in Member States that do not have a tradition of a risk-based approach to AML/CFT might also incur additional costs to employ or train competent staff to assess and manage ML/TF risk. For competent authorities, Option 2.2 would create the highest costs, as the assessment of diverse approaches to comply with Regulation (EU) 2023/1113 may be complex and requires supervisors to have access to experts able to exercise sound judgement on the adequacy of PSPs'/CASPs' systems and controls.

The advantage of Option 2.3 is that it sets clear expectations in cases where prescription is necessary and proportionate (for example in relation to checking if information contained in a transfer is missing or obviously meaningless) while at the same time allowing PSPs/IPSPs and CASPs/ICASPs to make risk-based decisions on the most appropriate and effective way to comply with Regulation (EU) 2023/1113, where the size and nature of PSPs/IPSPs' and CASPs/ICASPs'

business might justify different approaches. For PSPs/IPSPs and CASPs/ICASPs, Option 2.3 might create some one-off costs when adjusting their systems and controls and costs to employ or train staff in the application of the risk-based approach, where this approach is new. For competent authorities, the same considerations apply as in Option 2.2, whereas the costs are mitigated in the cases in which PSPs/IPSPs and CASPs/ICASPs are restricted to a prescriptive approach.

Option 2.3 is the retained option. It combines the benefits of non-standardised approaches for PSPs/CASPs and benefits of a prescriptive approach for competent authorities. PSPs/IPSPs and CASPs/ICASPs will benefit from being able to tailor their risk identification and management systems and controls to their own risk profile. Option 2.3 supports the EBA's objective to draft proportionate and effective guidelines on identifying transfers of funds and crypto-assets with missing or incomplete information and taking appropriate follow-up action, because this option is conducive to a common approach in those areas where consistency and regulatory certainty are needed, while at the same time allowing PSPs/IPSPs and CASPs/ICASPs some flexibility in the way they design and implement the systems and controls to comply with Regulation (EU) 2023/1113.

Overall, the benefits from these Guidelines are expected to outweigh potential costs and these Guidelines are expected to contribute to making the fight against ML/TF more effective.

4.2. Feedback on the public consultation

The EBA publicly consulted on the draft Guidelines on preventing the abuse of funds transfers and certain crypto-asset transfers for ML/TF (Travel Rule Guidelines). The consultation period lasted for three months and ended on 26 February 2024. A total of 33 responses were received, of which 26 were published on the EBA's website.

This section presents a summary of the key points arising from the consultation responses. The feedback table provides further details on the comments received, the analysis performed by the EBA triggered by these comments and the actions taken to address them, where action was deemed necessary. 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 most appropriate.

The EBA made changes to the draft Guidelines as a result of the responses received during the public consultation.

Summary of key issues and the EBA's response

Respondents welcomed the proposed Travel Rule Guidelines and commended the EBA for standardising approaches to the application of the travel rule requirements in respect of both transfers of funds and transfers of crypto-assets. In particular, respondents appreciated the EBA clarifying the type of information that should accompany the transfer, guidance on the interoperability of CASPs' systems, and the acknowledgment of technical limitations on messaging systems.

Respondents also identified points where the Guidelines could benefit from further clarification or alignment with other standards. These points related to:

- differences between the FATF's proposed revision of Recommendation 16, market developments and the EU's regulatory approach;
- interaction with MiCAR and the grandfathering clause;
- requirements on CASPs and transfers of crypto-assets (and specifically self-hosted wallets) in comparison to PSPs and transfers of funds;
- fostering interoperability;
- interaction with the Instant Payments under SEPA Regulation (EU) No 260/2012 (as amended by Regulation (EU) 2024/886);
- different interpretations of Article 4(1), point (c), and Article 14(1), point (d).

Differences between the FATF's proposed revision of Recommendation 16 and the EU approach

Some respondents perceived differences between the EBA's proposed approach and that of the FATF's revision of Recommendation 16. They argued that the EBA's guidelines should align with the future FATF standards on Recommendation 16.

These Guidelines set out how institutions should comply with the requirements in Regulation (EU) 2023/1113. Regulation (EU) 2023/1113 reflects the FATF standards that were in force when the Regulation was adopted. Since then, the FATF has initiated a review of Recommendation 16 and consulted on proposed amendments to this Recommendation. These amendments, if adopted, may require changes to Regulation (EU) 2023/1113 and, consequently, the content of these Guidelines.

Interaction between Regulation (EU) 2023/1113, these Guidelines and MiCAR's grandfathering clause

Some respondents asked to clarify whether Regulation (EU) 2023/1113 and these Guidelines will apply to entities that stand to benefit from MiCAR's grandfathering clause.

MiCAR introduces uniform EU market rules for a wide range of CASPs. At the same time, Regulation (EU) 2023/1113 amends the AMLD and extends the scope of the EU's AML/CFT regime to all CASPs. Like MiCAR, Regulation (EU) 2023/1113 will apply from 30 December 2024. This means that from 30 December 2024 CASPs as defined in MiCAR will be subject to the EU's AML/CFT regime and, therefore, these Guidelines. VASPs that are already subject to AML/CFT requirements because they fall within the scope of the AMLD or a domestic AML/CFT regime will continue to be subject to the applicable AML/CFT requirements. VASPs that are not yet subject to AML/CFT requirements will have to apply for MICAR authorisation to continue to operate in the EU from 30 December 2024 and will then also become obligated entities under the AMLD.

Requirements on CASPs and transfers of crypto-assets (and specifically self-hosted wallets) in comparison to PSPs and transfers of funds

Several respondents considered that the proposed Guidelines unfairly targeted crypto-assets, and specifically self-hosted wallets. They said that traditional financial instruments carried a higher inherent ML/TF risk than crypto-assets. According to them, aspects of the proposed Guidelines (1) failed to consider the fundamental right to privacy enshrined in the General Data Protection Regulation (GDPR) and Universal Declaration of Human Rights, undermined the safety and security of EU citizens in the digital realm and exposed them to greater risk of crime, including hacking, phishing or other types of online fraud; (2) weakened consumer protection and compromised financial inclusion as they seemed to discourage the use of self-hosted wallets; and (3) risked stifling innovation and economic growth of the blockchain and digital asset industry in the EU.

Regulation (EU) 2023/1113 sets out the rules CASPs must follow to mitigate financial crime risk and to ensure that transactions can be traced, whilst complying with data protection requirements. Recital 58 of this Regulation highlights 'the potential high risks associated with, and the technological and regulatory complexity posed by, self-hosted addresses'.

The Guidelines set out the steps institutions should take to comply with these rules. In line with Recital 58, they recognise that transactions with self-hosted addresses entail inherently higher risk

than transactions between two CASPs due to the unregulated nature of these tools and, in particular, the lack of identification and verification requirements applicable to the holders of self-hosted addresses. As such, these Guidelines reflect, and build upon, provisions in the Level 1 text.

Fostering interoperability

Respondents also stated that, in their view, interoperability between multiple travel rule tools did not reduce coverage gaps. Instead, requiring interoperability between travel rule tools would lead to lower standards overall, as tools would have to cater to whichever tool had the lowest security and privacy standards. The EBA notes that not all protocols on the market currently are interoperable as they often adopt different standards to comply with the travel rules. This may impact travel rule rollout and be resource-intensive where counterparties are able to comply with the transfer requirements only by integrating multiple protocols. Regarding possible lower standards created by interoperability, the Guidelines set out how CASPs should cater to security and privacy standards. If a protocol is not sufficiently robust to enable CASPs to comply with Regulation (EU) 2023/1113 (and in particular Articles 25 and 26) and these Guidelines, then CASPs should not be using it.

Interaction with the Instant Payments under SEPA Regulation (EU) No 260/2012 (as amended by Regulation (EU) 2024/886)

Some respondents considered that SEPA Regulation (EU) No 260/2012 (as amended by Regulation (EU) 2024/886) does not require real-time monitoring of instant credit transfers in euros, and asked whether the EBA will modify its current Guidelines to acknowledge this.

The limited application of the verification of whether payers and/or payees are subject to targeted financial restrictive measures as set out in Article 5d of SEPA Regulation (EU) No 260/2012 (as amended by Regulation (EU) 2024/886) 'is without prejudice to actions taken by PSPs in order to comply with restrictive measures (…) with Union law on the prevention of money laundering and terrorist financing' (see also Recital 26 of that Regulation). Therefore, the provisions on instant payments do not affect the requirement, under Regulation (EU) 2023/1113, to monitor transactions in line with these Guidelines.

Different interpretations of Article 4(1), point (c), and Article 14(1), point (d)

Respondents asked for clarification on the intention of Article 4(1), point (c), and Article 14(1), point (d), of Regulation (EU) 2023/1113 and amendments of the Guidelines. Relatedly, respondents stated that the definition of address appears to include things that are not typically associated with an address (e.g. official personal identification number and customer identification number) and some existing payment infrastructures do not support such data. This will create inconsistencies in the technical implementation of payment message formatting and it may be difficult to practically and meaningfully include the additional data attributes like official personal document number and customer identification number in a payment message, along with the address. Equally, countries such as the UK and US do not require payments to contain all the data points set out in the previous paragraph 26. As such, if EU PSPs are required to monitor and suspend/reject payments that do not include all this information, the result will be disruption of legitimate payments into the EU to the

detriment of the soundness of the financial system and of EU consumers and businesses, and it will place EU PSPs at a competitive disadvantage.

The EBA staff highlight that Regulation (EU) 2023/1113, in Articles 4 and 14, leaves space for interpretation, as does its predecessor, which is reflected in the responses to the 2022 Call for Input. Therefore, to foster convergence of practices, the EBA included guidance on how best to identify what information should be transmitted with the transfer considering all the data points referred in the Level 1 text. Based on the feedback received, the draft was amended to include a more flexible approach and to cater better for cross-border transfers. Adequate application of this provision is important for a number of reasons, namely to ensure that complete information will be submitted fulfilling the traceability purpose, that the payer/originator can be identified with a sufficient level of certainty, and that screening requirements can be addressed.

Other comments received are included in the following compliance table:

Comment	Summary of responses received	EBA analysis	Amendments to the proposals
General comment	Three respondents noted that the proposed Guidelines are silent on the due diligence requirement on relationships between CASPs, or counterparty due diligence as required by Recital 60 of Regulation (EU) 2013/1113.	Guideline 8 of the EBA ML/TF Risk Factors Guidelines (EBA/GL/2024/01) explains how firms should identify risks associated with counterparties and the type of CDD measures they should apply to mitigate these risks.	No change.
General comment	Several respondents suggested that the EBA offer guidance to firms on compliance with Regulation (EU) 2016/679 (GDPR).	Recital 19 of Regulation (EU) 2023/1113 states that 'the processing of personal data under this Regulation should take place in full compliance with Regulation (EU) 2016/679 (...)' and, equally, that 'the transfer of personal data to a third country is required to be carried out in accordance with Chapter V of Regulation (EU) 2016/679'. There are also other data protection mandates in the second paragraph of Article 25(4) of this Regulation which are separate from the ones addressed in these Guidelines.	No change.
General comment	One respondent stated that currently there are no effective systems or centralised infrastructure in place for CASPs to ensure that the required level of information is transferred and stored, and it would be useful to publish guidelines on the use of infrastructures and how they should be implemented.	Regulation (EU) 2023/1113 does not require a centralised infrastructure to collect, transfer and receive data. The EBA recognises that CASPs' systems are maturing and provides a period of adaptation, as explained in the former paragraph 13 (now 24). In addition, the Guidelines explain in Section 4.3. the expectations on those systems.	No change.
General comment	One respondent asked for the introduction of IBAN checks as other legislative acts are now doing (e.g. PSD3 and the Instant Payments Regulation).	Regulation (EU) 2023/1113 does not require the payer's PSP to systematically check that the name of a payee and the IBAN transmitted correspond. Nevertheless, PSPs will have to carry out these checks if they are subject to legislation that requires this.	No change.
2. Subject matter, scope and definitions			
General comment	One respondent stated that it should be clarified that where banks/PSPs are not providers of crypto services and only carry transactions from or to CASPs for their customers (not offering crypto services themselves), those entities must apply the	Compliance with Chapter II or III of Regulation (EU) 2023/1113 depends on the role that the entity plays in the transfer and is clarified directly in the Level 1 text. Namely, Article 2(1) of Regulation (EU) 2023/1113 states that 'this Regulation shall apply to transfers of funds (…) which are sent or received by a payment service provider or an intermediary payment service provider (…).' Or 'it shall also apply to transfers of crypto-assets (…) where' it involves a	No change.

	relevant requirements in Chapter II of Regulation (EU) 2023/1113 but not CASPs' requirements in Chapter III.	'crypto-asset service provider, or the intermediary crypto-asset service provider (…).'	
Para. 6 of JC/GL/2017/16	One respondent noted that a PSP depicts a broader concept of a regulated entity type, while a payer's PSP, IPSP and payee's PSP depict a certain role played by that PSP. The same seems to refer to a CASP and ICASP. The respondent suggested clarifying whether the intention of mentioning the IPSP paired with the PSP was only to stress that a certain provision does not only refer to the first and last PSP in a transfer chain, but to all of them.	The concepts of PSP, IPSP, CASP and ICASP are defined in Regulation (EU) 2023/1113. A payer's PSP, IPSP, payee's PSP, originator's CASP, ICASP and beneficiary's CASP are different due to the role they play in the transfer ecosystem. The EBA uses the same definitions in these Guidelines.	No change.
4.2. Exclusion from the scope of Regulation (EU) 2023/1113 and derogations			
General comment	Two respondents suggested clarifying whether rejected, returned or recalled transfers of funds (R-transactions) constitute a new transfer of funds within the meaning of Article 3 of the Regulation, or not, and hence whether the requirements in these Guidelines should apply or not to such R-transactions.	According to Regulation (EU) 2023/1113, a '"transfer of funds" means any transaction at least partially carried out by electronic means on behalf of a payer through a payment service provider, with a view to making funds available to a payee through a payment service provider (…)'. Therefore, where the PSP intention with a processing task is not to make the funds available to a payee, then the requirements of Regulation (EU) 2023/1113 do not apply.	No change.
General comment	One respondent requested clarification on whether transaction fees (gas fees) are out of the scope of the Guidelines.	According to Regulation (EU) 2023/1113, a '"transfer of crypto-assets" means any transaction with the aim of moving crypto-assets from one distributed ledger address, crypto-asset account or other device allowing the storage of crypto-assets to another, carried out by at least one crypto-asset service provider acting on behalf of either an originator or a beneficiary (…)'. Therefore, transaction fees do not qualify if they intend to be a payment for a service. However, reference to transaction fees is relevant to determine, for instance, whether the self-hosted address in transfers above EUR 1 000 is owned or controlled by the CASP's customer. In this case, the CASPs should not consider the transaction fees (namely gas fees and similar).	Para. 68 (now 81) amended.

		The EBA Guidelines set out how institutions should comply with their legal obligations and do not duplicate the Level 1 text. The exclusions stated in Article 2(2) of Regulation (EU) 2023/1113 mean that the transactions that fall within those specific situations and conditions are not required to have the information transmitted with the transfer.	
General comment	One respondent noted that the Guidelines do not refer to exclusions listed in Article 2(2) of the Regulation (EU) 2023/1113, and it is unclear what information should accompany such transactions. The respondent stated that ML/TF risks could exist in those cases and that this was particularly relevant in the instances foreseen in the exclusion in Article 3, point (b), of Directive (EU) 2015/2366 as it may be confused with transfers 'on behalf of'.	The EBA highlights that the transfers 'on behalf of' situations are different from the ones referred to in Article 3, point (b), of Directive (EU) 2015/2366. Recital 11 of Directive (EU) 2015/2366 is clear in clarifying that 'the exclusion should apply when agents act only on behalf of the payer or only on behalf of the payee, regardless of whether or not they are in possession of client funds. Where agents act on behalf of both the payer and the payee (such as certain e-commerce platform), they should be excluded only if they do not, at any time enter into possession or control of client funds.' A commercial agent has the legal authority to conclude the sale or purchase of goods or services on behalf of the payer or the payee only if they have the authority to affect the legal relations of the client, who is the payer or the payee, with third parties and to bind the payer or payee to a purchase or sale of goods or services. This would not be fulfilled simply by providing the technical means by which a payer places or a payee accepts an order.	Para. 3 (now 15) amended.
4.2.1. Determining whether a card, instrument or device is used exclusively to pay for goods or services (Article 2(3), point (a), and (5), point (b), of Regulation (EU) 2023/1113)			
Para. 4, 21, 22, 26, 29 and 43	Three respondents asked for clarification of the role of a payer's PSP, IPSP and the payee's PSP.	The paragraphs refer to specific articles in Regulation (EU) 2023/1113 which themselves apply to different actors. The Guidelines follow this approach and have been amended to clarify that CASPs and PSPs need to establish which role they play in the payment and crypto-asset transfer chain.	New para. 12 added.
Para. 4 and 5	Seven respondents considered that the analysis of customers' trends and behaviours to determine whether the card is used for payment for goods or services would require PSPs to monitor card payments in real time and will require major technical development for all PSPs, incurring great financial costs. The focus should be on the functionality of cards, instruments and devices instead.	The EBA has amended Guideline 2.1 to clarify that an ex ante assessment of the functionality of cards, instruments or other devices is necessary to benefit from the exemption in Article 2(3)(a) of Regulation (EU) 2023/1113.	Para. 4 and 5 (now 16) amended.

	Two respondents requested clarification of what falls within the category of goods and services through real life examples. For instance, whether the purchase of FX currencies and an associated transfer of funds in another country would be considered a service. One respondent asked for clarification on what should be considered an instrument as this might vary in different national frameworks.	The trading of international currencies and currency derivatives does constitute a payment for goods or services for the purpose of Regulation (EU) 2023/1113. Regarding the third comment, an instrument refers to an electronic money instrument.	
4.2.2. Linked transfers in relation to the EUR 1 000 threshold (Article 2(5)(c), Article 5(2), Article 6(2) and Article 7(3) of Regulation (EU) 2023/1113)			
General comment	One respondent said that there is a lack of definition of what constitutes 'linked' transactions in Section 2.2.	Section 2.2. (now Section 4.2.2.) describes the criteria that constitute a linked transaction.	No change.
Para. 7(b)	Six respondents asked for clarification regarding the short timeframe to be considered. Five respondents requested clarification regarding the scope of 'related persons' and stated that it is neither practical nor reasonable for PSPs to identify payers or payees that are 'linked', for example through family or professional connections, when they have only one of the parties as a customer. Relatedly, one respondent stated that linked persons are not stored, and the analysis may impact the processing time of all transactions. One respondent asked for clarification on whether 'commercial relationships' are included in the definition (for example, invoices payment).	Regarding the first comment, in line with the risk-based approach underpinning the EU's AML/CFT framework, it is for each PSP/CASP to determine what a reasonable 'short' timeframe is, given their business model and the level of ML/TF risk to which their business is exposed. This is because placement, layering and integration can vary considerably depending on the delivering channels, geographies, customers and products/services. Regarding the second comment, it is not the EBA's intention to request the filtering of family or professional connections where those are not parties to the transfer. Therefore, the Guidelines have been amended for clarity. The concept of a linked transfer is, however, relevant where the PSP manages multiple accounts for the same customer or connected customers, or there is a risk that transfers are sent to multiple accounts belonging to the same person.	Para. 18(b) (now 18(b) and (c)) amended.
Para. 8(c)	Two respondents indicated that the inclusion of 'smurfing techniques' at this point leads to ambiguities. Equally, this would lead to a flood of transactions to be checked.	Robust AML/CFT systems and controls entail policies and procedures to detect attempts to circumvent thresholds. The paragraph was amended for further clarity.	Para. 8(c) (now 19(c)) amended.

Para. 6 to 9	One respondent suggested identifying definitions and criteria applicable to the risk management policies set out in the consultation paper. One respondent asked whether simplified due diligence (SDD) measures are expected to determine whether there is intentional fragmentation and, if so, whether it will be relevant to ascertain if there are related transfers in a continued period in time. One respondent observed that linked transfers in the context of crypto-asset transfers are not mentioned in the Regulation or the Guidelines. It would be beneficial to clarify if and how these should be taken into account.	Regarding the first comment, based on Section 4.2.2. of these Guidelines, PSPs have to determine this based on the information they have available both when funds transfers are initiated and ex post. With respect to the second comment, EBA/GL/2021/02 provides that SDD should only be applied in specific cases where the ML/TF risk has been assessed as low and to the extent permitted by national legislation. It is clear that SDD is not an exemption from any of the CDD measures. Regarding the intentional threshold circumvention, this should indeed be part of the CDD, as reflected in the Guidelines. On the third comment, there is no equivalent provision for CASPs because Recital 30 of Regulation (EU) 2023/1113 is clear that all crypto-asset transfers are subject to the same requirements regardless of their amount and of whether they are domestic or cross-border transfers. Nevertheless, as part of the CDD measures and in a risk-based approach, CASPs are encouraged to apply the same considerations to identify threshold circumventions for the EUR 1 000 requirements. Amendments were introduced for further clarity.	Para. 6 to 9 (now 17 to 20) amended.
4.3.1. Messaging or payment and settlement systems			
General comment	One respondent said that it would be relevant to clarify the terminology used to ensure a consistent interpretation of requirements, thereby allowing for greater standardisation, referring to the lack of a specific definition of 'messaging systems' in Guideline 3.1 including ambiguity in the use of the terms 'payment and settlement' and 'transfer and settlement' systems.	The EBA has aligned the Guidelines with the wording used in Regulation (EU) 2023/1113.	Throughout the document amendments have been made to standardise the text and align with the language used in the Level 1 text, i.e. 'messaging or payment and settlement system'.

Para. 10	One respondent stated that infrastructures and services for the transfer of funds that are devoid of any technical limitations do not exist in practice and that this will impact compliance with the Guidelines. One respondent stated that the requirement that a PSP should be fully capable of transmitting and receiving the information might be hard to fulfil with certain schemes. The respondent is of the view that it should be clearly stated that this obligation applies 'unless there are restrictions in the message format used'. Equally, when the message format does not allow the full length of a message, guidance should be provided on how the information should be prioritised.	While the EBA agrees that infrastructures and services that are devoid of any technical limitations do not exist in practice, the EBA clarifies in the Guidelines that PSPs, IPSPs, CASPs and ICASPs that cannot ensure that their systems are able to transmit, receive or convert the information without error or omission should not use those systems as is. In addition to not being in compliance with the Regulation, it entails serious operational risks that ultimately impact the robustness of AML/CFT controls. On the second point, the Guidelines already provide guidance on how the information should be prioritised to comply with the Level 1 text when the message format does not allow the full length of information.	No change.
Para. 11	Two respondents stated that the paragraphs could be misread as to enable a messaging system, which could be a third party, to be able to access unencrypted personal data of the customers. The respondents suggest emphasising the importance of data protection obligations when personal data traverses across multiple systems. Two respondents stated that it should be clarified that adherence to industry data standards can mitigate the risks associated with handling varying data formats and the potential for errors and omissions. Both respondents provided different examples of specific, widely recognised standards that, in their view, ensure consistency in both the structure and content of data payloads. One respondent considers that this paragraph fails to recognise practical challenges that arise from the use of different systems, across different jurisdictions, where differing formats are used that have varying levels of capacity to include information. While the respondent supports the premise aimed at maintaining data integrity, the respondent	The intention of paragraph 11 is to acknowledge two points: (1) technical limitations, which means data-related constraints, boundaries or shortcomings that arise from the technological components, systems and frameworks involved in the processing of transfers; (2) the need to use several, possibly non-interoperable, messaging or payment and settlement systems to address information transfer requirements and to transact with counterparties. This can create data integration issues and hamper institutions' ability to comply with travel rule requirements. Notwithstanding these limitations and challenges, Regulation (EU) 2023/1113 is clear that no exemptions apply. It is therefore incumbent upon PSPs, IPSPs, CASPs and ICASPs to ensure that their systems are sufficiently robust to enable them to comply with their legal requirements. For clarity, the EBA amended the draft. Articles 25 and 26 of Regulation (EU) 2023/1113 set out how personal data should be protected as it traverses multiple messaging or payment and settlement systems. Regarding the reference to industry standards, the EBA highlights that the Guidelines do not recommend a particular solution.	Para. 11 (now 22) amended.

	considers that the language as drafted is not aligned to industry practice.		
Para. 12	Two respondents suggested referring to the EBA Guidelines to clarify the interlinks with the broader IT systems and what is required in the context of outsourcing arrangements.	The EBA has included a reference to Guidelines EBA/GL/2019/02.	Para. 12 (now 23) amended.
Para. 13	Two respondents stated that the current draft may give rise to misinterpretation that non-compliant protocols, systems and practices are accepted. They suggest making clear that technical limitations should be only temporary. Four respondents stated that achieving full compliance for CASPs within the proposed timeframe appears challenging. For them, the transitional period should be extended to at least the end of 2025, as most CASPs will not yet operate under full MiCAR authorisation in July 2025. They consider that, in the meantime, the use of other infrastructures or services to comply with Regulation 2023/1113 should be acceptable. Two respondents stated that this period should also be extended to PSPs/IPSPs in relation to transfers of crypto-assets. For example, e-money institutions issuing EMTs will need to comply with the new rules under the recast FTR for EMT transfers, in which case they should also be able to benefit from the transition period that applies to CASPs. One respondent asked for confirmation on whether the transitional period also applies to batch transfers, and if they can, during that period, test different methods to find out the most effective approach to comply with this requirement.	On the first and second comment, the EBA stresses that non-compliance with Regulation (EU) 2023/1113 is not accepted. The Guidelines recognise that technical limitations may exist but must be temporary. Alternative infrastructures or services to comply with Regulation 2023/1113 are acceptable only during the transitional period. After that time, infrastructures or services should be fully capable of transmitting the required information as set out in these Guidelines. The draft has been amended for clarity. Regarding the third comment, the transitional period for technical solutions is only for crypto-asset (as defined in Article 3(14)) transfers because they are newly introduced to the requirements. That transitional period applies to all CASPs providing crypto-asset transfers. Article 3(15) of Regulation (EU) 2023/1113 defines a 'crypto-asset service provider' as 'a legal person or other undertaking whose occupation or business is the provision of one or more crypto-asset services to clients on a professional basis, and that is allowed to provide crypto-asset services in accordance with Article 59'. Accordingly, the entities listed in Article 59, in conjunction with Article 60, of Regulation (EU) 1114/2023 – which are entities authorised as a CASP or credit institution, central securities depository, investment firm, market operator, electronic money institution, UCITS management company, or an alternative investment fund manager that is allowed to provide crypto-asset services pursuant to Article 60 – are considered CASPs for the purposes of these Guidelines where they provide crypto-asset transfers. This includes transfers of EMTs and ARTs. With respect to the fourth comment, the transition period envisaged in the Guidelines refers to all the technical-related provisions that CASPs/ICASPs will have to apply. During that period, CASPs/ICASPs can test different methods to find out the most effective approach to comply with this requirement in a manner that is consistent with AML/CFT objectives.	Para. 13 (now 24) amended.

Para. 14(b)	Four respondents stated that it is necessary to submit the required information as soon as possible, but no later than the moment of the transfer itself (in the VA context, the initiation of the blockchain transaction), aligning with the FATF approach.	The EBA amended the Guidelines to clarify when the information on the crypto-assets should be transferred.	Para. 14(b) (now 25(b)) amended.
Para. 15(a)	Three respondents requested further clarity on the intention of the reference to 'both within and outside CASPs and ICASPS'. Four respondents recommended advising CASPs to take a holistic approach when adopting a messaging tool, which would include considering whether the tool appropriately prioritises data privacy and security, effective governance over the use of their tools, and broad global coverage. Overemphasis on seamless communication without accompanying technical standards and security requirements could force CASPs to adopt less secure, but more interoperable networks. Two respondents stated that systems specific to a CASP may differ greatly from another CASP, depending on several factors including sizing. For example, if a CASP only conducts very limited business activity connected with a particular CASP, it may not even need to adopt a third-party messaging protocol or have a single messaging protocol connected with every CASP's system. One respondent stated that even if a CASP uses a solution that is technically interoperable with a closed travel rule protocol, the CASP will be unable to exchange information with its members unless they secure membership in that protocol. On this matter, the FATF has clarified that the due diligence process should be conducted autonomously and independently by each VASP and that the need for network-	Regarding the first comment, the paragraph was amended for clarity. On the second and third comment, the EBA clarifies that the Guidelines do not provide rules for the selection of tools or mandate the adoption of specific tools, but rather set out criteria that should be taken into consideration during selection. Although smaller players or channels with reduced business volumes might not need to resort to an external, third-party protocol, it is expected that a solution will be needed. Equally, as stated by the FATF 2023 Target Update, 'interoperability will also enable VASPs to lower compliance costs by reducing the need for acquiring multiple compliance tools'. If a protocol is not interoperable (amongst others and according to the concept described in the Guidelines) then the CASP (the originator's and the beneficiary's) shall not choose to work with it. Relatedly, on the suggestion about reachability metrics, the EBA sees merit in including it in the criterion as it can complement the accuracy of checks. In addition, clarity has been introduced with regard to the applicable Level 1 articles to which the Guidelines refer in Section 4.3. Regarding the fifth comment, the EBA has aligned the narrative to the language in the Level 1 text.	Para. 15 (now 26) amended.

	level control of membership should not obstruct interoperability efforts. One respondent suggested differentiating a protocol from a technical solution. The former is a set of rules for formatting and exchanging data so that all parties can process it. The latter can enable communication through the use of a single travel rule protocol, several, or none – in the case of CASPs using just email, for instance.		
4.3.2. Multi-intermediation and cross-border transfers			
Para. 16	One respondent stated that while there will be instances where the payment chain is under the control of, or at least fully visible to, the PSP/IPSP, there will also be many instances where this is not the case, particularly for cross-border transfers.	The paragraph refers to the role of the PSP and IPSP concerning the transfer to the next PSP or IPSP. The PSP and IPSP should have visibility of how the information is transmitted, as referred in the Level 1 text.	No change.
Para. 17	One respondent noted that there seems to be an assumption that an IBAN and/or BIC indicates a country, which is not correct. As a solution, the respondent suggested clarifying that, in cases of cross-border transfers or in cases of doubt, the transfer should be deemed to constitute a cross-border transfer, resulting in the use of appropriate payment channels that may facilitate the necessary transmission of information. Two respondents stated that the PSPs are not in a position to ensure that information is actually received by the next PSP in the transfer chain and it does not represent the actual industry practice. Relatedly, one respondent indicated that suggesting that PSPs/IPSPs should ensure that the next PSP in the transfer chain receives the information on payer and payee can be construed as a requirement to un-batch all batch payments, and for the information on underlying payers and payees to be passed on to the next PSP.	PSPs must have systems and controls in place to distinguish between domestic and cross-border transfers, based on information they have available. The EBA agrees that, in cases of doubt, the transfer should be considered cross-border and amended the Guidelines in this regard. On the second comment, this paragraph does not impose an un-batching of transfers. However, the need to ensure the transmission of information as described in the guidance of para. 17 should prevail to ensure adequate assessment of ML/TF risks.	Para. 17 (now 28) amended.

Para. 18	Two respondents seek additional guidance as they find the obligations imposed on PSPs and IPSPs to be unclear in this paragraph.	The paragraph aims to prevent circumventions of responsibilities for the purpose of AML/CFT, namely related to exclusions.	No change.
Para. 19	Six respondents suggest that the Guidelines go against the principle of a batch transfer. In practice, an IPSP is not settling the individual underlying parties but merely facilitating and passing on bundled funds from the originating PSP to the beneficiary PSP for the settlement (disbursement). The responsibility for complying with the FTR in the scenario of batch transfers should be clarified and placed on the payer rather than the intermediary PSP as it is not technically feasible for IPSPs to collect such details and still efficiently perform their roles as intermediaries without disrupting the flow of funds. It could create challenges in the payment system. One respondent states that the guideline misses the view of the card business. Visa and Mastercard do not support such alternative mechanisms, thus making such requirements for card issuing PSPs impossible to comply with.	According to Regulation (EU) 2023/1113, compliance is the responsibility of the payer's PSP, IPSP and payee's PSP. The payer's PSP has certain responsibilities which also include the capture, verification and retention of information. For batch transfers, the text clearly indicates in Article 11(2)(c) that IPSPs 'shall implement effective procedures, including, where appropriate, monitoring after or during the transfers, in order to detect whether the (…) information on the payer or the payee is missing (…) for batch file transfers where the payment service provider of the payer or of the payee is established outside the Union, the information referred to in Article 4(1), points (a), (b) and (c), and Article 4(2), points (a) and (b), in respect of that batch file transfer'. Nevertheless, bearing in mind the IPSPs' technical limitations, the narrative was amended to ensure clarity and the focus is now on the role of the IPSP rather than on the payer's PSP or originator's CASP, as in the consultation version.	Para. 20 (now 31) amended.
4.4. Information to be transmitted with the transfer in accordance with Articles 4 and 14 of Regulation (EU) 2023/1113			
General comment	One respondent stated that, in addition to LEI and country codes (ISO 3166), there are several technical standards that can be leveraged for digital assets as the consistent use of standards is the foundation of achieving transferability across multiple payment platforms (e.g. ISO 4217:2015, ISO 24165, amongst others).	Other technical standards can also be used to the extent that they would enable the PSP to comply with the Regulation.	No change.
Para. 20	Three respondents stated that the term 'error' should be clarified, as it appears to be too broad and could include situations that are not relevant to the systematic reporting of errors.	Regarding the first comment, those paragraphs refer to the errors relevant to the acquisition of the information required by Articles 4 and 14 of Regulation 2023/1113. A clarification has been added to the paragraph. On the second and third comments, Articles 4 and 14 of Regulation (EU) 2023/1113 provide that the payer's PSP and originator's CASP should verify	Para. 20 (now 31 and 32) amended.

	Two respondents requested clarification that the originator's CASP should not be held liable where the next CASPs in the transfer chain do not fulfil the relevant requirement to obtain the missing information if it was already informed by the originator's CASP that an error had occurred. One respondent asked for clarification of whether, when the initial submission is changed, the payer's PSP still needs to submit any missing info to the intermediary via an alternative channel mechanism as envisaged in para. 19. One respondent asked for clarifications on what actions could be considered sufficient to detect meaningless, missing or incomplete information. In practice, the only way to make the required detection after the payment is processed is to resubmit the payment through the end-to-end payment process within the bank.	the accuracy of the information before the transfer. If an error is detected after the transfer, the whole payment chain should be made aware and each PSP and CASP involved in the transfer should ensure the transfer is in compliance with the Level 1 text. On the fourth comment, Articles 7, 11, 19 and 20 state the specific obligations to detect missing information which should be fulfilled by the next PSP/CASP in the transfer chain. These Guidelines also provide further details in Sections 4.5. and 4.6. If necessary, if there is no other technical solution (including alternative channel mechanisms), the transfer can be recalled - to the possible extent -and resent with the correct information.	
4.4.1. Providing the payment account number of the payer in accordance with Article 4(1), point (b), of Regulation (EU) 2023/1113, and of the payee (Article 4(2), point (b), of Regulation (EU) 2023/1113)			
Para. 21	Two respondents consider that, when a wire transfer is used, there are no card payments within the end-to-end process. There is no current technical way to include card numbers in SEPA or SEPA Instant payments. One respondent noted that, in addition to the IBAN and card number, a broad range of other identifiers unambiguously representing an account exist. One respondent stated that when a PSP is instructed to make a payment to a certain IBAN, it is not transparent to earlier PSPs in the chain whether this IBAN indicates the final, single payment account and whether this account is held by the PSP associated with that IBAN. Virtual IBANs (VBANs) are also often used as well, and they indicate who the funds are meant for, rather than the number of that payee's account.	Concerning the first and second comments, the EBA highlights the scope of Regulation (EU) 2023/1113 which applies, amongst other things, when a payment card is used in order to effect a transfer of funds or electronic money tokens between natural persons acting as consumers for purposes other than trade, business or professional activity. Also, with respect to transfers of funds within and to outside the Union, a variety of payment systems that facilitate payments in and between countries exist. It is important to ensure standardisation in line with the requirement in the Level 1 text, which is why the EBA retained the original guidance. On the third comment, the EBA acknowledges that PSPs may be unable to distinguish IBANs from vIBANs and has highlighted this in its *Report on virtual IBANs* (EBA/Rep/2024/08). The EBA considers that compliance with the Regulation is ensured if the PSP can demonstrate that it has taken reasonable	No change.

		steps to be able to identify discrepancies that may suggest that a vIBAN is being used, and if so, to follow up as necessary.	
4.4.2. Providing the name of the payer, the payee, the originator and the beneficiary respectively in accordance with Articles 4(1), point (a), 4(2), point (a), 14(1), point (a), and 14(2), point (a), of Regulation (EU) 2023/1113			
Para. 22	Four respondents asked for clarification of whether the transitional period is also applied to PSPs.	The transitional period refers to the transfer of crypto-assets only because PSPs have been subject to these requirements since 2017 and the substance of these requirements, and the EBA's guidelines for PSPs, have not changed.	No change.
Para. 22(a)	One respondent stated that this goes beyond the text of the recast FTR, which uses the phrase 'on the basis of documents, data or information obtained from a reliable and independent source'. It would be helpful if requirements could allow for some flexibility in relation to evidence, as customers wishing to initiate a transfer may not always have their government-issued ID to hand.	Information can also be verified using electronic identification means which meet the requirements of the eIDAS Regulation. The text was amended to reflect this.	Para. 22(a) (now 35(a)) amended.
Para. 22(b)	One respondent argued that the trade name cannot replace the legal name. In the case of technical limitations, a truncation of the legal trade name would be a preferable solution, also considering that this hypothetical situation seems very unlikely to happen; the number of characters that can admit this information in the payment messages is usually quite extensive.	The EBA agrees the trade name cannot replace the legal name. A business's legal name is the official name that appears on government and legal forms. A trade name is what a business uses to operate and interact with customers. The Guidelines are clear that the trade name is only to be transmitted as a last resort and only when technical limitations exist and provided that it can unequivocally be traced back to the legal person and match any such names recorded in official registries. To support this, the LEI or any available equivalent official identifier also play a role.	No change.
Para. 22(c)	Three respondents stated that the addition of 'the names of all holders of the account, address or wallet' introduces a major technical change for the payment processes, which is expected to be costly and time-consuming.	If, according to Article 3(3) of Regulation (EU) 2023/1113, more than one person holds a payment account and allows a transfer of funds from that payment account, or, where there is no payment account, gives a transfer of funds order, then all the names should accompany the transfer.	No change.
4.4.3. Providing the address of the payer and of the originator including the name of the country, official personal document number, and customer identification number or, alternatively, the date and place of birth of the payer in accordance with Articles 4(1), point (c), and 14(1), point (d), of Regulation (EU) 2023/1113			

General comment	Three respondents stated that the Guidelines seem to introduce new requirements as they require that the payer's PSP / originator's CASP share sensitive personally identifiable information, which not only presents privacy and security concerns but also goes beyond the Level 1 text.	This paragraph refers to the provisions contained in Articles 4 and 14 of Regulation (EU) 2023/1113.	No change.
Para. 23	Four respondents suggested that the wording should be aligned to the future AMLR to ensure that the addresses that are included with the transfer of funds are the verified address. Three respondents indicated that, for legal entities, the principal place of business should be preferable as the registered address in several countries does not give an indication of the actual location of the legal entity and might be the address of a law firm office or corporate service provider without any connection to the actual legal entity. Two respondents argued that, in relation to all DLT refinements, the draft Guidelines should include criteria and georeferencing forecasts of the DLT itself.	With respect to the first comment, the EBA agrees that consistent language should be applied transversally across both Level 1 and Level 2 texts. The text has been amended for alignment. Regarding the second comment, providing the principal place of business only could create ambiguity, as a company may have different places of business. The text has been amended to reflect the AMLR and focus on both the registered and official office. With respect to the third comment, the information to accompany the transfer is defined in Articles 4 and 14 of Regulation (EU) 2023/1113. The EBA Guidelines aim to further clarify those points but cannot go beyond that.	Para. 23(a) (now 36(a)) amended. Para. 23(b) (now 36(b)) amended.
Para. 24	Two respondents observed that in some countries there is no indication of a street number, street name, city, postal code, or country as a component of an address. Therefore, country and city should be the compulsory information and the other components of the address could be considered optional. One respondent asked for clarification on the meaning of 'to the extent possible'. One respondent stated that LEIs are associated with known correct mailing addresses for legal entities. Individuals who present vLEIs have had to present government-issued credentials such as a passport, which includes an address that the government already vetted, and this would be an asset for the Guidelines.	Regarding the first and second comments, as stated in the paragraph, to the extent possible means that PSPs and CASPs will attempt to fill the fields as much as possible. This means as permitted by the messaging or payment and settlement system and the jurisdictional particularities. On the third comment, Regulation (EU) 2023/1113 allows the possibility to include LEIs and, therefore, it is understood that this can encompass verifiable LEIs.	No change.

Para. 25	Three respondents stated that there are also addresses designated as a P.O. box or 'poste restante' for safety reasons, as stipulated in the national law of certain Member States (e.g. individuals at risk due to their professions who have received personal threats or threats against their families; individuals facing domestic dispute situations may require special protection due to the threat of violence). In such cases, the bank may be aware of the actual residence of these individuals, but in accordance with national law it is obliged to keep this information confidential.	Those cases are covered under specific national regimes.	No change.
Para. 26	Nine respondents asked for clarification on the intention of Articles 4(1)(c) and 14(1)(d) of Regulation (EU) 2023/1113 and amendments of the Guidelines to reflect their interpretations. Relatedly, three respondents stated that the definition of address appears to include things that are not typically associated with an address (e.g. official personal identification number and customer identification number) and some existing payment infrastructures do not support such data. This will create inconsistencies in the technical implementation of payment message formatting and it may be difficult to practically and meaningfully include the additional data attributes like official personal document number and customer identification number in a payment message, along with the address. Equally, peer countries such as the UK and US do not require payments to contain all the data points set out in paragraph 26. As such, if EU PSPs are required to monitor and suspend/reject payments that do not include all this information, the result will be disruption of legitimate payments into the EU to the detriment of the soundness of the financial system and of EU consumers and businesses, and it will place EU PSPs at a competitive disadvantage. Three respondents stated that there is no requirement in the Level 1 text on assessing the quality of data from the	With respect to the first comment, Regulation (EU) 2023/1113, in Articles 4 and 14, seems to leave space for interpretation, reflected in the responses to the 2022 Call for Input exercise. Therefore, the EBA included guidance on how best to identify what information should be transmitted with the transfer considering all the data points referred in the Level 1 text. The draft was changed to a more flexible approach and to cater for the nuances of cross-border transfers. Adequate application of this provision is important for a number of reasons, namely to ensure that complete information will be submitted fulfilling the FTR purpose, that the payer/originator can be identified with a sufficient level of certainty, and that screening requirements can be addressed. The EBA also points out that the information items are clearly stated in Articles 4 and 14 and the messaging or payment and settlement systems should technically allow compliance with Regulation (EU) 2023/1113. Regarding the second comment, the three terms refer to different meanings. The 2009 Basel Committee on Banking Supervision document *Due diligence and transparency regarding cover payment messages related to cross-border wire transfers* refers to 'manifestly meaningless or incomplete', which, although complementary, is different from an unambiguous identification of the payer. With respect to the third comment, following the FATF approach, the customer identification number refers to a number that uniquely identifies the originator to the originating financial institution and is a different number from	Para. 26 (now 39) amended.

	perspective of the 'unambiguous identification' and asked for clarification on the meaning as it is perceived as subjective. It was suggested that wording from the 2009 Basel Committee on Banking Supervision be used. Three respondents asked for a definition of the customer's identification number.	the unique transaction reference number. The customer identification number must refer to a record held by the originating financial institution which contains at least one of the following: a national identity number, or a date and place of birth.	
Para. 27	One respondent stated that ambiguity arises when the term 'joint accounts' might also refer to legal entities or organisations rather than individual persons. In such cases, clarification becomes essential to distinguish whether the term applies exclusively to individuals or if it encompasses the possibility of shared ownership by legal entities such as companies, partnerships or other organised entities.	A joint account is an account opened by at least two people (called joint holders) to facilitate the management of common expenditure in which each co-holder can operate the account with only a signature and the means of payment can be used by any co-holder. If the natural or legal persons fall under this definition then it would be within the scope of the paragraph.	No change.
4.4.4. Providing an equivalent identifier to the LEI of the payer, the payee, the originator and the beneficiary in accordance with Articles 4(1), point (d), 4(2), point (c), 14(1), point (e), and 14(2), point (d), of Regulation (EU) 2023/1113			
Para. 28	Two respondents requested that it be specified whether with the indication 'subject to the existence of the necessary field in the relevant payments message format […]' the requirement only applies to the type of messaging systems that dedicate a specific/structured field to the LEI code. Relatedly, one respondent understood that as long as the messaging system does not have a dedicated field for the LEI, or its equivalent, it is not required to provide the LEI or its equivalent. Two respondents asked that it be specified if the 'BIC' code can be considered as an equivalent official identifier of the LEI code. One respondent asked if it is correct to assume that any other identifiers, that are not automatically issued but can be	With respect to the first comment, an LEI or alternative identifier is only required to be provided where 'the necessary field in the relevant payments message format' exists, as clarified in the Level 1 text. Regarding the second comment, the EBA is aware that a BIC is widely used in the industry as a universal identifier code in certain systems. However, a BIC does not fulfil the criteria described in the paragraph as it refers to the unique ID assigned to banks in their group and cannot be used as an alternative identifier, in the absence of an LEI. Conversely, the IBAN can be used as an alternative to the account number. On the third comment, the EBA has amended the text to clarify that it also caters to situations where the identifier is not issued immediately. With respect to the fourth comment, the items should be cumulative and a clarification was inserted.	Para. 28(c) (now 41(c)) amended.

	assigned later (e.g. tax ID), are not considered as LEI equivalents. One respondent requested clarification as to whether all the criteria listed are required or whether the items can be taken as a list of alternatives.		
4.5.1. Procedures to detect missing information in accordance with Articles 7, 11, 16 and 20 of Regulation (EU) 2023/1113			
Para. 29	One respondent stated that, when handling incomplete information, it would be valuable to recognise that variances in compliance requirements across jurisdictions can lead to instances where data, while aligned with the originating CASP's local regulations, may not fully meet the standards outlined in the Level 1 text. One respondent observed that the concept of 'adequate' should be clarified regarding possible real-time or ex post monitoring of operations with possible missing information.	On the first comment, European CASPs are bound by the requirements set by Regulation (EU) 2023/1113 which makes no distinction between crypto-asset transfers within, or from outside, the Union, as explained in Recital 27. Regarding the second comment, this concept is clarified in Section 4.5.3., which refers to the EBA's Guidelines on ML/TF risk factors.	No change.
4.5.2. Admissible characters or inputs checks on transfers of funds in accordance with Articles 7(1) and 11(1) of Regulation (EU) 2023/1113			
Para. 30(c)	Three respondents suggested amending the guideline to reflect established mechanisms and allow for systems with business rules or other means of assistance on how to proceed when inadmissible characters or inputs are detected.	These guidelines do not rule out the use of systems that accommodate business rules or other means of assistance on how to proceed when inadmissible characters or inputs are detected.	No change.
4.5.3. Monitoring of transfers in accordance with Articles 7(2), 11(2), 16(1) and 20 of Regulation (EU) 2023/1113			
Para. 33	Two respondents stated that Articles 7(2) and 11(2) of the FTR refer to 'monitoring after or during transfers', not to monitoring before and during transfers as is being proposed.	The Guidelines refer to specific articles in Regulation (EU) 2023/1113, as indicated in each subsection. For clarity, the EBA is amending the paragraph to align with the wording of the Level 1 text.	Para. 33 (now 46) amended.
Para. 34	Two respondents believe it is more effective to assess a combination of risk-relevant factors, rather than imply or require that all of them be considered.	On the first comment, in line with the EBA's approach to AML/CFT, the intention is not to require entities to use all risk factors but instead to identify	Para. 34 (now 47) amended.

	One respondent stated that it is crucial to stress the importance of understanding not only the counterparty risk but also the data handling practices in alignment with Regulation (EU) 2016/679 (GDPR). The Guidelines would benefit from addressing the need for CASPs to implement robust systems and controls for the handling of personal data to ensure GDPR compliance across all parties involved in the transfer chain.	those that are pertinent to their business. The paragraph has been amended for clarity. Regarding the second comment, these requirements are set out in the Regulation itself.	
Para. 34(c)	One respondent requested clarification on whether the EBA is referring to jurisdictions that are on the FATF's grey list or blacklist as the way it is currently drafted risks resulting in a divergent approach.	The current wording reflects both lists, as the FATF places jurisdictions on the grey list when the jurisdiction is under increased monitoring due to non-compliance with FATF recommendations, and on the blacklist when it has serious strategic deficiencies in countering ML/TF and proliferation.	No change.
Para. 34(d)	One respondent asked whether there is a publicly available list of which countries have not yet implemented the travel rule obligation. One respondent stated that, although they acknowledge the risks associated with PSPs/CASPs in countries not adhering to FATF recommendations, they are concerned that this criterion might result in a situation of de-risking. It is not the role of institutions to regularly assess the implementation of FATF country recommendations.	PSPs and CASPs should refer to publicly available information, including lists of compliance with Recommendation 16 published by the FATF.	Para. 34(d) (now 47(d)) amended.
Para. 34(e)	One respondent stated that, at present, it is not possible to fully identify and differentiate a hosted or self-hosted wallet. One respondent stated that, with regard to transfers involving entities based in a third country that does not enforce a licensing regime or does not regulate CASP activity, they disagree that this should be a determining factor for enhanced monitoring. Geography and maturity of the domestic AML regime should be taken into account, but it should not be the main or determining criterion.	On the first comment, Regulation (EU) 2023/1113 is clear that certain requirements apply to self-hosted wallets. CASPs should identify those wallets as described in Section 4.8.1. Regarding the second comment, as reflected in the Guidelines, PSPs and CASPs should adopt a risk-based approach, including a holistic view of all relevant risk factors.	No change.

Para. 34(g)	One respondent observed that 'anonymity-enhancing techniques, products, or services' does not represent a unified category, but a spectrum of techniques, products and services, only a segment of which represents ML/TF risk-increasing factors.	Privacy-enhancing technologies (PETs) and anonymity-enhancing technologies (AETs) serve different purposes and provide different levels of privacy protection. They are often used interchangeably but, for the purpose of these Guidelines, they are considered as two different concepts. PETs are a broad category of technologies and practices aimed at safeguarding individuals' personal information and data. They focus on minimising data collection, limiting data sharing and ensuring that data is used only for its intended purpose while preserving the functionality of the service or system. They are, therefore, useful for the purpose of addressing data protection requirements and the challenges with data sharing. AETs, on the other hand, are a subset of PETs that specifically focus on concealing or obfuscating a user's identity online. These technologies aim to provide a high degree of anonymity, often by dissociating online activities from an individual's real-world identity. They might be, for instance, used to obfuscate the origin of funds or the true originator. The guideline refers only to anonymity-enhancing techniques and not to privacy-enhancing technologies, considering that the anonymity-enhancing techniques present higher ML/TF risks, as also reflected in the ML/TF Risk Factors Guidelines.	No change.
4.5.4. Missing information checks in accordance with Articles 7 (2), 11 (2), 16 (1) and 20 of Regulation (EU) 2023/1113			
Paras from 37 to 39	One respondent suggests providing guidance on how to determine whether some information is 'inconsistent' as the introduction of new terminology contributes to hindering consistency in the application of requirements. Three respondents would welcome further clarification on the resulting possible courses of action for PSPs.	The paragraph was amended to align with the wording in the Level 1 text.	Para. 37 (now 49) amended.
4.6.2. Rejecting or returning a transfer in accordance with Articles 8(1), point (a), 12, point (a), 17(1), point (a), and 21(1), point (a), of Regulation (EU) 2023/1113			
Para. 42	Three respondents stated that, despite being aware that the Level 1 text uses the term 'reject' multiple times, the term does not accurately reflect a feasible option for transfers involving crypto-assets, as in the absence of intermediaries	Regarding the first comment, there may be situations where the recipient is first notified about a transaction even before the transaction is technically processed on the blockchain. In this case, there may be a 'rejection' by the	New para. 55 added.

	there is no acceptance or rejection of a transaction. It is suggested that terms such as 'return' or 'not making the crypto-asset available to its client' be used. One respondent questioned who would be responsible for paying the fee associated with the return of crypto-assets (e.g. gas fee). The respondent asked if it is possible to deduct both the operational costs and the network fees that the CASP should incur for the return from the crypto-assets of the transferor. Equally, in the case of disputes, what liabilities could be attributed to the CASP for not completing the transfer or for reversing the crypto-assets. One respondent highlighted that currently guidance on a return policy does not exist. This leads to VASPs adopting various practices on return policies as most VASPs operate aggregated wallets (usually, hot wallets) to process multiple users' withdrawal requests. If travel rule compliance needs to be applied to the return transaction, sending the transfer back to the originator may not be feasible since there is no guarantee that the originator (not a user of the VASP) has an account amongst the approved VASPs.	beneficiary CASP. For the cases where this is not possible, the guideline already provides a 'return' option. Nevertheless, a clarification was inserted. On the second comment, the general current practice in the market is that the party initiating the return (in this case, the CASP) bears the associated costs. However, this can vary depending on the specific terms and conditions agreed upon between the CASP and its clients. It may be possible for the CASP to deduct operational and network fees from the transferor's crypto-assets, provided this is clearly communicated and agreed upon in the service terms. Regarding the third comment, guidance was included in the Guidelines to address this issue.	
4.6.3. Requesting required information in accordance with Articles 8(1), point (b), 12(1), point (b), 17(1), point (b), and 21 (1), point (b), of Regulation (EU) 2023/1113			
Para. 43	Five respondents indicated that requests for information turnaround times can be affected by e.g. the number of parties in a payment flow, language differences between those parties, time zone differences and the presence of non-working days.	With respect to the first comment, the paragraph already envisages longer deadlines. However, to reflect the impact of the complexity of the transfer landscape, the deadline has been extended to seven days.	Para. 43 (now 56) amended.
Paras 43 and 44	One respondent is concerned that the paragraph does not leave room for ex post monitoring as it suggests that the transfer is necessarily suspended before processing and does not recognise the possibility of ex post monitoring and review.	The text has been clarified and amended to align with the Regulation.	Para. 43 (now 56) amended. Para. 44 (now 57) amended.

Para. 45	Three respondents stated that there is a contradiction between the guideline and Articles 8(2) and 12(2) of Regulation (EU) 2023/1113 which stipulate the possible courses of action and the rejection of payments is just one possibility.	The text has been clarified and amended to align with the Regulation.	Para. 45 (now 59) amended.
Para. 48	One respondent suggested clarifying what volume of transactions would be considered to be sufficient to apply paragraphs 48(a) and/or 48(b).	With respect to the first comment, that should be in a risk-based approach as defined in Section 4.6.1.	No change.
Para. 55	One respondent noted that the requests for missing information or clarification about a transfer involving a self-hosted address should affect only the transfer made from a self-hosted address and not the transfer made to a self-hosted address. In the former case, the request should be sent directly to the customer, whereas in the latter case there should be no request for information, as in such cases the CASP should neither initiate nor execute the transfer after a missing and/or incomplete information assessment.	Para. 55 (now 47 and 52) refers to Articles 8(1), 12, 17(1) and 21(1) of Regulation (EU) 2023/1113. All these articles provide for the obligations of the beneficiary's CASP in the case of a transfer from a self-hosted address. In these cases, as noted by the respondent, if there is some missing information CASPs must acquire it from their customer/beneficiary before deciding on executing the transfer. The Guidelines follow the same principle as expressed in Recital 39 of Regulation (EU) 2023/1113.	No change in substance. Now paras 58 and 63.
4.6.4. Executing a transfer in accordance with Articles 8(1), 12(1), 17(1) and 21(1) of Regulation (EU) 2023/1113			
Paras 49 and 50	Three respondents stated that Articles 8, 12, 17 and 21 of Regulation (EU) 2023/1113 allow CASPs the flexibility to execute transfers under certain conditions, basing the decision on their risk assessment procedures instead of fixed criteria. By foreseeing the unambiguous identification of the parties as a mandatory criterion, the Guidelines introduce a stricter framework than that prescribed by the Level 1 text. This situation is problematic because due to the sunrise period and interoperability limitations there remains a significant percentage of transactions lacking the necessary information.	The Guidelines allow for a risk-based approach as does the Level 1 text. However, it is a basic principle of AML/CFT that the entity should know the customer it is dealing with.	No change.
4.7.1. Treatment of repeatedly failing PSPs, CASPs, IPSPs or ICASPs in accordance with Articles 8(2), 12(2), 17(2) and 21(2) of Regulation (EU) 2023/1113			

Para. 59	One respondent stressed that it would be both inefficient and ineffective to leave individual PSPs/CASPs to determine the criteria as to when entities should be considered to be 'repeatedly failing' and, if so, what action should be taken. The EBA should set out both the criteria for categorising institutions as 'repeatedly failing' institutions and actions for remediation.	These Guidelines already clarify the criteria for categorising institutions as 'repeatedly failing' which should be both qualitative and quantitative. It equally clarifies the actions for remediation and the last resort steps, following the approach of Regulation (EU) 2023/1113.	No change.
4.7.2. Reporting repeatedly failing PSPs, CASPs, IPSPs or ICASPs to the competent authority in accordance with Articles 8(2), 12(2), 17(2) and 21(2) of Regulation (EU) 2023/1113			
Para. 62	One respondent stated that the last part on reporting repeatedly failing entities to national competent authorities seems to contradict (previous) paragraphs 56, 57 and 58 which allow PSPs to consider a combination of quantitative and qualitative criteria for assessing whether or not a PSP or IPSP is repeatedly failing.	The paragraphs are not contradictory. Despite the fact that the failing PSP/IPSP/CASP/ICASP provides an explanation, the purpose of the reporting is for the competent authority to monitor compliance with provisions.	No change.
Para. 63	One respondent stated that this information is not encompassed within the travel rule sharing data. It should be considered that this information might not be available to the PSP/IPSP/CASP/ICASP.	The information required to be notified to the authorities is not travel rule data. It refers to the analysis of the activity with the counterparty and is the result of an analytical process which is available to the PSP/IPSP/CASP/ICASP.	No change.
4.9. Transfers of crypto-assets made from or to self-hosted ad-dresses in accordance with Articles 14(5) and 16(2) of Regulation (EU) 2023/1113			
General comment	Two respondents stated that an important factor in ensuring the smooth execution of transaction flows may be the whitelisting of addresses or the creation of a centralised register for suspicious wallets, particularly in relation to self-hosted wallets.	Regulation (EU) 2023/1113 does not foresee a centralised register for suspicious wallets.	No change.
4.8.2. Identification of a transfer from or to a self-hosted address			
Paras 65 and 66	Two respondents stated that the market has a shortage of 'advanced analytics tools' and 'other suitable technical means' that can be used to monitor this and are costly, and the	On the first comment, Regulation (EU) 2023/1113 has specific requirements if a transfer of crypto-assets is made from or to a self-hosted address. CASPs must therefore determine whether they will be transacting with another CASP	New para. 78 added.

	requirement is unnecessary. In addition, the receiving centralised wallets may not be completely capable of identifying or verifying the accuracy of transactions from self-hosted wallets without both the CASP and the consumer being severely encumbered by this requirement. If the requirements are not applied proportionately, this may risk circumventing broader regulatory standards by using non-EU-compliant/regulated CASPs for transfers. Two respondents asked for more guidance on the data that could be collected from customers related to the presence and identity of a counterparty, including trading names, brand names, legal entity names or legal entity identifiers. Two respondents stated that the Guidelines should specify if CASPs are required to unequivocally determine the type of wallet prior to completion of the transaction, as at present it is unclear at what stage the data exchange should occur for transactions with a self-hosted wallet.	or with a self-hosted wallet and the EBA has clarified the steps CASPs should take. On the second comment, where the transfer is made to or from another CASP, the originator's CASP and the beneficiary's CASP should take the necessary steps to accurately identify the counterparty CASP. A clarification was inserted. Regarding the third comment, the Level 1 text states that 'the information shall be submitted in advance of, or simultaneously or concurrently with, the transfer of crypto-assets and in a secure manner and in accordance with Regulation (EU) 2016/679.' The EBA in guideline 14 further clarifies that the required information should be transmitted immediately (meaning prior to or simultaneously or concurrently with the transfer itself) and securely and no later than the initiation of a blockchain transaction. Specifically on self-hosted wallets, the Level 1 text does not foresee a different timeframe and, therefore, should be considered the same.	
4.8.3. Identification of the originator and beneficiary in a transfer from or to a self-hosted address			
Para. 67	Six respondents noted that paragraph 67 is not in line with the risk-based approach outlined in Article 19(a) of AMLD5 and that the verification requirement for transactions below EUR 1 000 is not in line with the FTR (for transactions below EUR 1 000, the FTR requires only the collection of information, but not the verification). Two respondents explained that collecting information from the customer to identify the self-hosted wallet of the originator or beneficiary might not be feasible in some situations. One respondent noted that the verification requirement is technically unfeasible, as the identity of the originator or	The requirement addresses Article 19a of the AMLD, as amended by Regulation (EU) 2023/1113. To better reflect the requirement on the identification vs verification, the EBA has amended the Guidelines, also making reference to the mitigating measures commensurate with the risks identified. Collecting the information, in these situations, from the customer is as recommended in Recital 39 of Regulation (EU) 2023/1113. Regarding the comment on the use of blockchain analytics, the text gives space for flexibility in the verification of non-customers.	Para. 67 (now 80) amended.

	beneficiary cannot be verified by cross-matching data with blockchain analytics.		
4.8.4. Transfers above EUR 1 000 and proof of ownership or controllership of a self-hosted address			
Para. 68	One respondent recommended clarifying the timing of the evaluation of the transaction amount.	A reference is added for clarity.	Para. 68 (now 82) amended.
Paras 69 and 71	Eight respondents stated that the majority of the methods for verification of ownership outlined would require efforts to be made by CASPs and hinder competition with non-EU CASPs, and this burden would be further exacerbated if a combination of more than two methods is required, and operationally this would be very challenging to achieve. Included in this, one respondent noted that, in many cases, there will not be two viable methods for the verification of ownership of SHWs, especially for Unspent Transaction Output (UTXO) such as Bitcoin. Four respondents indicated that CASPs could be required to use additional measures: only one method on its own is not sufficiently reliable to ascertain the ownership or control of the self-hosted address, and the adoption of additional methods improves the degree of reliability of that verification. One respondent also suggested allowing for a whitelisting process for future transactions involving wallets that have previously been identified as belonging to the client. Whereas two respondents suggested ensuring the ownership of self-hosted wallets to be on an ongoing basis, not just one time. Two respondents suggested removing/rewording items e) and f), as they seem to refer to the same technical means.	On the first comment, CASPs have the flexibility to choose a method of verification of ownership/controllership of a self-hosted address beyond what is set out in these Guidelines. The Guidelines were, however, amended to focus on one method, considering its effectiveness and risk assessment. If one method adequately determines ownership/controllership, it suffices. Additional methods are required only if doubts persist. With regard to the second comment, that requirement is already mirrored in the Guidelines. Regarding the third comment, the EBA is of the view that under the risk-based approach a whitelisting process could be helpful and foster efficiency as long as adequate controls are put in place. The text has been amended with a balanced approach to reflect this. On the fourth comment, the EBA agrees that only one should be kept and deleted e).	Para. 69 (now 83) (e) deleted. Para. 70 (now 84) added point (c). Section 4.8.5 amended.
Para. 72	Four respondents noted that it is not in line with the risk-based approach implied by Article 19a of AMLD5 and with Articles 14 and 16 of the recast Regulation (EU) 2023/1113, which require		Section 4.8.5. amended.

	CASPs only to verify the identity of their own customers and to apply mitigating measures. One respondent requested clarification regarding the regulatory expectation regarding transactions exceeding EUR 1 000 between CASPs and third-party self-hosted wallets, as those are not covered in the FTR. One respondent noted that Article 19a requirements do not specify whether the self-hosted wallets are held by the CASP's customer or a third party. They should therefore be regarded as applying to both, not only to third parties, as stated in paragraph 72.	The EBA has amended the Guidelines to clarify this point.	
Paras 67, 69 and 72	Six respondents proposed a unification and clarification of the terms concerning 'blockchain analytics', 'advanced analytical tools' and 'blockchain analytic data'.	The terms are placed in context across the Guidelines and are in the EBA view self-explanatory.	No change.
4.8.5. Mitigating measures to put in place regarding transfers from or to a self-hosted address			
Para. 73	One respondent asked for clarification, as the fact that a transfer involves a self-hosted address alone is not grounds for EDD.	The paragraph does not state that any transfer involving self-hosted wallets is to be considered as high-risk from an ML/TF point of view. It merely sets out how the risk assessment is to be carried out and what needs to be taken into account.	No change.
4.9. Obligations on the payer's PSP, payee's PSP and IPSPs where a transfer is a direct debit			
Para. 75	Three respondents noted that, by mentioning only the provision of the payee's information, the guideline misses the aspect that provision of the payer's information commences on the payee's side as part of the direct debit collection.	The EBA has clarified the text based on the suggestions received.	Para. 75 (now 91) amended.
Impact assessment			
General comment	One respondent was concerned that Option 1.1 seems to advantage PSPs/IPSPs already regulated by the EU ML/TF	Option 1.1. vs 1.2 refer to the scope of the mandate in terms of the articles that the Guidelines should cover, not to the extent that the Level 1 text	No change.

	framework in terms of one-off costs incurred, over CASPs/ICASPs, as its interpretation is that the text states that the costs for PSPs/IPSPs are expected to be absorbed by the modifications of the underlying ML/TF framework but does not reference the implications for CASPs/ICASPs.	obligations are applied to PSPs/IPSPs and CASPs/ICASPs. The EBA recognises the costs for both PSPs/IPSPs and CASPs/ICASPs in adapting to the further standardisations introduced by these Guidelines, as mandated by Regulation (EU) 2023/1113. The paragraph provides the caveat that PSPs/IPSPs were already subject to the Level 1 requirements and, therefore, will have to focus on the modifications of the underlying ML/TF framework, but not on the foundational implementation (like CASPs/ICASPs will).	