EBA/CP/2023/35

24.11.2023

Consultation Paper

Guidelines

on preventing the abuse of funds and certain crypto-assets transfers for money laundering and terrorist financing purposes under Regulation (EU) 2023/1113

('The Travel Rule Guidelines')

Contents

1. Responding to this consultation

The EBA invites comments on all proposals put forward in this paper.

Comments are most helpful if they:

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

Submission of responses

To submit your comments, click on the 'send your comments' button on the consultation page by 26.02.2023. Please note that comments submitted after this deadline, or submitted via other means may not be processed.

Publication of responses

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

Data protection

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

2. Executive Summary

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 is proposing to deliver 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 remains, therefore, relevant and has been maintained in the consultation draft.

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

[1] JC/GL/2017/16

3. Background and rationale

Background

On 26 June 2015, Regulation (EU) 2015/847 on information accompanying transfer 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 fund 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 transfer. The objective was to prevent the abuse of fund 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 presents the same ML/TF risks as the transfer of funds.

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

Articles 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.

Rationale

Through these draft Guidelines, the EBA aims to promote 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 they should be applied. A common understanding is essential to ensure the consistent application of EU law. It is also conducive to a stronger European AML/CFT regime.

Before drafting the consultation version of 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 its review of the 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 draft Guidelines

This Section explains the rationale for provisions in the draft 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 for the payment of 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 for the payment of goods and 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 proposed Guidelines set 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

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.

can be included in the transfer. Technical limitations can hamper the transfer of information and make compliance with Regulation (EU) 2023/1113 difficult.

To address this, the proposed Guidelines set out common standards of information PSPs and CASPs should include in relevant fields when transferring crypto-assets and funds. They also set out the steps CASPs and ICASPs should take if the full information cannot be transmitted due to technical limitations.

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

C. Guidelines 3.1. on the interoperability of protocols

Specifically with transfers of crypto-assets, several protocols exist to address information transfer requirements, including open-network protocols, closed-network protocols and protocol-agnostic solutions. Not all protocols are interoperable, which means that CASPs might have to use multiple protocols 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 draft Guidelines highlight that a protocol'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 CAPs including the risk that transfers with complete information could also be unnecessarily rejected.

To address this, the draft Guidelines set out common standards on information that PSPs and CASPs should include in the name, address, and LEI/alternative identifier fields for crypto and fund 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 draft 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 their 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];

- EBA DRAFT Guidelines on internal policies, procedures and controls to ensure the implementation of Union and national restrictive measures under Directive (EU) 2013/36 and Directive (EU) 2015/2366

- 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];

[4] EBA/GL/2021/02

[5] EBA/GL/2022/05

- EBA Guidelines on outsourcing arrangements[6]; and
- EBA Guidelines on ICT and security risk management[7].

[6] EBA/GL/2019/02

[7] EBA/GL/2019/04

EBA/GL-REC/20XX/XX

DD Month YYYY

4. Draft Guidelines

on preventing the abuse of funds and certain crypto-assets transfers for money laundering and terrorist financing purposes under Regulation (EU) 2023/1113 ('The 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[8]. 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/202x/xx'. Notifications should be submitted by persons with appropriate authority to report compliance on behalf of their competent authorities. Any change in the status of compliance must also be reported to EBA.

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

[8] 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 mandates to issue guidelines in accordance with Article 36 first and second subparagraph of Regulation (EU) 2023/1113[9].

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 effective procedures to detect and manage transfer 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) specifies technical aspects of the application of Regulation (EU) 2023/1113 to direct debits.

7. In addition, these Guidelines aim at addressing the mandate to issue guidelines in accordance with Article 19a(2) of Directive (EU) 2015/849 [10] 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;

[9] 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.

[10] 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 Directive (EU) 2015/2366 have the same meaning in the Guidelines. Further, 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, PSP, IPSP, CASPs and ICASPs identify, assess, and understand the ML/TF risks to which PSP, IPSP, 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 from the payer or originator to the payee or beneficiary.

3. Implementation

Date of application

10. These Guidelines apply from 30.12.2024.

Repeal

11. The following Guidelines are repealed with effect from 30 December 2024: JC/GL/2017/16.

4. Preventing the abuse of funds and certain crypto-assets transfers for money laundering and terrorist financing purposes

1. General provisions

Transfer of funds and crypto-assets

1. PSPs, IPSPs, CASPs and ICASPs should ensure that their procedures referred to in Articles 7(1 and 2), Article 8(1), Article 11(1 and 2), Article 12(1), Article 16(1), Article 17(1), Article 20 and Article 21(1) of Regulation (EU) 2023/1113 are regularly reviewed, improved where necessary, and kept up to date.

2. PSPs, IPSPs, CASPs, and ICASPs should regularly review whether the procedures as implemented are effective, for example, by testing a random sample from all processed transfers.

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

Transfer of funds and crypto-assets

3. This Section provides guidance for PSPs and CASPs on how to determine whether the conditions for the application of the exclusions or derogation provided in Regulation (EU) 2023/1113 are met.

2.1. Determining whether a card, instrument or device is used exclusively for the payment of goods or services (Article 2(3) point (a) and (5) point (b) of Regulation (EU) 2023/1113)

Transfer of funds

4. For PSPs to determine whether a card, instrument or device is exclusively used for the payment of goods or services, PSPs should make, at least, the following assessments:

    a. identify the use of any merchant categorisation codes, including payment card schemes' Merchant Category Code (MCC), that is used to categorise the type of goods or services sold;

b. determine whether the payer or payee is engaged in an economic or professional activity, irrespective of its legal form, using information collected for the purpose of Article 13 of Directive (EU) 2015/849, if available, or information accessible via third party providers or in publicly available sources; and

c. analyse, where available, trends and behaviours, including transfer history and patterns to determine whether the payer makes payments for goods or services, or the payee receives payments for goods or services.

Transfer of crypto-assets

5. For CASPs to determine whether a card, instrument or device is exclusively used for the payment of goods or services, CASPs should make, at least, the following assessments:

a. Identify the use of any categorisation code assigned to customers that categorises the type of goods or services sold;

b. determine whether the originator or beneficiary is engaged in an economic or professional activity, irrespective of its legal form, using information collected for the purpose of Article 13 of Directive (EU) 2015/849, if available, or information accessible via third party providers or in publicly available sources; and

c. analyse, where available, trends and behaviours, including transfer history and patterns, to determine whether the originator makes payments for goods or services, or the beneficiary receives payments for goods or services.

2.2. Linked transfers in relation to the 1000 EUR threshold (Article 2(5)(c), Article 5(2), Article 6(2) and Article 7(3) of Regulation (EU) 2023/1113)

Transfer of funds

6. PSPs should have policies and procedures in place to detect transfers that appear to be linked in line with the further specifications set out in this Section.

7. 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 or persons linked with them, within a short timeframe; or are sent from one payer to different payees or different payers to the same payee or persons connected with them within a short timeframe.

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

a. the timeframe they will apply for different types of transfers, based on the risk assessments they have carried out in line with the "EBA's ML/TF Risk Factors Guidelines"[11];

[11] EBA/CP/2023/11

b. the criteria for the identification of linked transfers;

c. how they will identify attempts to circumvent the threshold, including the possible use of smurfing techniques; and

d. whether and which other scenarios might also give rise to linked transactions.

9. The assessment of what constitutes linked transfers should be made, taking into account the moment the transfer was ordered or initiated and its absolute values, regardless of any charges levied by the PSP.

3. Transmitting information with the transfer (Article 4, Article 5, Article 6 and Article 14 of Regulation (EU) 2023/1113)

3.1. Messaging systems

Transfer of funds and crypto-assets

10. PSPs, IPSPs, CASPs and ICASPs should use infrastructures and services for the transmission and reception of information, fully capable of transmitting and receiving the information required under Regulation (EU) 2023/1113 without the need to resolve technical limitations in order to comply with that Regulation.

11. Where PSPs, IPSPs, CASPs and ICASPs use different protocols or messaging systems, they should ensure that their systems are able to convert information into a different format without error or omission and in a timely manner. Where a PSPs, IPSPs, CASPs and ICASPs cannot ensure that their systems are able to convert information into a different format without error or omission, the PSPs, IPSPs, CASPs and ICASPs should not use such systems.

12. PSPs, IPSPs, CASPs and ICASPs should use systems for the transfer of information that are secure as set out in the "EBA Guidelines on ICT and security risk management"[12].

Transfer of crypto-assets

13. By way of derogation from paragraph 10 and until 31 July 2025, CASPs and ICASPs may exceptionally use infrastructures or services that are not fully capable of transmitting the required information and require additional or alternative technical solutions in order to comply with Regulation (EU) 2023/1113, provided that they put in place additional policies and procedures to compensate for technical limitations, so that the CASP and ICASP can comply fully with Regulation (EU) 2023/1113. These policies and procedures should at least include alternative mechanisms for collecting, holding and making available to the next CASP or ICASP in the transfer chain the information that cannot be transmitted due to technical limitations.

[12] EBA/GL/2019/04

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

    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, before the transfer is completed or at the time of the transfer.

15. When choosing the messaging protocol, CASPs and ICASPs should ensure that the protocol's architectures are sufficiently robust to enable the seamless and interoperable transmission of the required information by:

    a. evaluating the protocol's interoperability features to ensure it can seamlessly communicate with other systems, both within and outside CASPs and ICASPs;

    b. considering the compatibility with existing industry standards, protocols, and blockchain networks to facilitate integration; and

    c. assessing data integration and data reliability.

3.2. Multi-intermediation and cross-border transfers

Transfer of funds

16. The PSPs and IPSPs, which enable the execution of transfers with two or more IPSPs or PSPs on cross-border basis, should describe in the 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.

17. For the purpose of the transfer of information, when the PSP or IPSP handling a transfer does not have a direct relationship with the payer, that PSP or IPSP should ensure that the next PSP in the transfer chain receive the information on the payer and payee. To that end the transfer chain (from end-to-end) should be considered as one and the flow of information on the original payer and payee preserved. Where the transfer is made from a cross-border channel to a domestic channel the domestic IPSPs or PSPs should assess whether the transfer is correctly identified as a cross-border transfer.

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

3.3. Batch transfers (Article 6(1), Article 7(2) (c), Article 15, Article 16(1), Article 20 of Regulation (EU) 2023/1113)

Transfer of funds and crypto-assets

19. Where a batch transfer is routed through one or more intermediaries and settled with limited underlying information, meaning that not all required information is relayed with the batch transfer to the intermediaries, the payer's PSP and originator's CASP should submit the missing information which is required, to the intermediary, 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. Information to be transmitted with the transfer (Article 4 and Article 14 of Regulation (EU) 2023/1113)

Transfer of funds and crypto-assets

20. When transmitting information, PSPs and CASPs should not change the initial submission, unless requested by the IPSP, payee's PSP, ICASP or beneficiary's CASP as part of the monitoring tasks to detect missing information under Article 7, Article 11, Article 19 or Article 20 of Regulation (EU) 2023/1113; or if, following the transfer, an error is identified by the payer's PSP or originator's CASP. Following the transfer, if an error has been identified by the payer's PSP or originator's CASP, the payer's PSP or originator's CASP should also inform the next PSP and CASP in the transfer chain. The next PSP and CASP in the transfer chain should then perform, once again, the necessary tasks to detect the missing or incomplete information.

4.1. Providing the payment account number of the payer (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

21. PSPs may treat the International Bank Account Number (IBAN) if available - or, where the transfer of funds is made using a payment card, the number of that card (including the Primary Account Number (PAN)) - as the payment account number, on condition that the number used permits the fund transfer to be traced to the payer or the payee.

4.2. Providing the name of the payer (Article 4(1) point (a) of Regulation (EU) 2023/1113), of the payee (Article 4(2) point (a) of Regulation (EU) 2023/1113), of the originator (Article 14(1) point (a) of Regulation (EU) 2023/1113), and of the beneficiary (Article 14(2) point (a) of Regulation (EU) 2023/1113)

Transfer of funds and crypto-assets

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

    a. For natural persons, the full official name of the customer as documented on an official and government-issued document (such as an identity card or passport), or if this 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"[13]. Where technical limitations exist, as referred to in paragraph 13, that do not permit the transmission of the full official name, the payer's PSP and originator's CASP should, at minimum, include the first official given name and last official surname, as per the official document.

b. For legal persons, the name under which the legal person is registered. Where technical limitations exist, as referred to in paragraph 13, that do not permit the transmission of the full registered legal name, the payer's PSP and originator's CASP should transmit the trading name. Trading names used should unequivocally be traced back 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 13, that do not permit the transmission of all names of all parties to the transfer, the payer's PSP and originator's CASP should transmit the name of the holder of the account, address or wallet who is initiating the transfer; or, where that is not possible, the primary account, address or wallet holder.

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

Transfer of funds and crypto-assets

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

a. For natural persons, the habitual residence of the payer or originator. In case of a vulnerable person as referred to in paragraph 19b of "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" and cannot reasonably be expected to provide an address in relation to their habitual residence, the PSP or the CASP may use an addresses that is provide in alternative documentation as referred to in that Guidelines paragraph 19(b), 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 or originator's registered office.

24. 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 Codes of Country 'the ISO 3166' (Alpha-2 or Alpha-3), postal code, city, state and province and municipality, street name, building number or building name.

[13] EBA/GL/2023/04

25. The payer's PSP and originator's CASP should provide the postal address as specified in paragraph 24. 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).

26. Where the information on the name, the account number, address and the official personal document number prevents the unambiguous identification of the payer or originator, the payer's PSP or the originator's CASP should transfer the information on the date and place of birth in addition to the address and official personal document number.

27. For transfers from a joint account, address or wallet, the information of all holders of the account, address or wallet. Where the transmission of the respective information of all the parties cannot take place due to technical limitations, as referred to in paragraph 13, 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. Providing an equivalent Identifier to the LEI of the payer (Article 4(1) point (d) of Regulation (EU) 2023/1113), of the payee (Article 4(2) point (c) of Regulation (EU) 2023/1113), of the originator (Article 14(1) point (e) of Regulation (EU) 2023/1113) and of the beneficiary (Article 14(2) point (d) of Regulation (EU) 2023/1113)

Transfer of funds and crypto-assets

28. The payer's PSP and the originator's CASP should consider only those official identifiers, which may be provided alternatively to the LEI 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, as equivalent which:

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

    b. are published in public registries;

    c. are automatically 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;

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

5. Detecting missing information (Article 7, Article 11, Article 16 and Article 20 of Regulation (EU) 2023/1113)

5.1. Procedures to detect missing information (Article 7, Article 11, Article 16 and Article 20 of Regulation (EU) 2023/1113)

Transfer of funds and crypto-assets

29. Procedures as referred to in Article 7, Article 11, Article 16 and Article 20, to be effective, should at least contain the following:

    a. a method 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 payee's PSPs, IPSPs, beneficiary's CASPs, and ICASPs are exposed, determined in accordance with "The EBA's ML/TF Risk Factors Guidelines";

    c. the criteria that alert to risk-increasing factors; and

    d. the obligations of members of staff to detect that information required by Regulation (EU) 2023/1113 is missing and the processes they should follow.

5.2. Admissible characters or inputs checks on transfers of funds (Article 7(1) and Article 11(1) of Regulation (EU) 2023/1113)

Transfer of funds

30. The payee' PSPs and IPSPs should use messaging or transfer and settlement systems ensuring that:

    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 and as further specified in Section 4 of these Guidelines;

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

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

31. Where a PSP's or IPSP's messaging or transfer and settlement system does not meet all the criteria set out in paragraph 30, the PSP or IPSP should put in place controls to fully mitigate the shortcomings.

32. Payee's 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 system or payment and settlement system have been filled using characters or inputs in accordance with the conventions of that system; and

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

5.3. Monitoring of transfers (Articles 7(2), Article 11(2), Article 16(1) and Article 20 of Regulation (EU) 2023/1113)

Transfer of funds and crypto-assets

33. The payee's PSPs, IPSPs, beneficiary's CASPs, or ICASPs should set out in their policies and procedures how to determine which transfers are appropriate to be monitored before the transfer takes place and which transfers are appropriate to be monitored during the transfer in accordance with Article 7(2), Article 11(2), Article 16 (1) and Article 20 by applying the following:

    a. taking into account all risk increasing factors, including those specified in the "EBA's Guidelines on ML/TF risk factors"[14], and any other risk factors identified at national (e.g. in the National Risk Assessment) and sectoral level (by competent authorities) or other factors identified by the entity that are relevant to their business; and

    b. identifying 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, as set out in this Section.

34. PSPs, IPSPs, CASPs and ICASPs should determine the risk increasing factors which are adequate to the specific products and services, customers, delivery channels and geographies based on "The EBA's ML/TF Risk Factors Guidelines". That list should at least include:

    a. transfers that exceed a pre-defined value threshold. When determining the threshold, PSPs and CASPs should take 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, the payer's PSP, originator's CASP, the payee's PSP or beneficiary's CASP are located in countries or territories that are subject to restrictive measures or 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, the payee's PSP or beneficiary's CASP is 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 not consistent with the Directive (EU) 2015/849 or

[14] EBA/GL/2021/02

the revised FATF Recommendations and countries which 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 is located in a country which has not yet implemented the obligation to obtain, hold, and transmit required originator and beneficiary information, immediately and securely, when conducting wire and virtual assets transfers, as per Recommendation 16 of the FATF.

e. transfers with entities based in a third country that does not have licencing regimes or does not regulate PSP/CASP activity, or with self-hosted addresses;

f. transfers from or to accounts, addresses or wallets known to be linked with suspicious activity;

g. anonymity-enhancing techniques, products, or services (including, but not limited to, mixers or tumblers, Internet Protocol (IP) anonymisers, stealth addresses) that hinder the tracing of crypto-assets by concealing the trail leading back to the originator have been used;

h. a negative AML/CFT compliance record of the prior PSP, IPSP, CASP or ICASP in the transfer chain, including as have been exposed in public lists;

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 techniques to perform layering of addresses;

k. funds and crypto-assets received and rapidly transferred further, thus artificially extending the transfer chain.

35. PSPs, IPSPs, CASPs and ICASPs' systems should be configured in a way that an alert is triggered should a risk increasing factor be detected while also looking for missing information.

36. PSPs, IPSPs, CASPs and ICASPs should note that missing or inadmissible information may not, by itself, give rise to suspicion of ML/TF. 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.

5.4. Missing information checks (Article 7 (2), Article 11 (2), Article 16 (1) and Article 20 of Regulation (EU) 2023/1113)

Transfer of funds and crypto-assets

37. 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 inconsistent.

38. 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').

39. 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.

6. Transfers with missing or incomplete information (Article 8, Article 12, Article 17 and Article 21 of Regulation (EU) 2023/1113)

6.1. Risk-based procedures for determining whether to execute, reject or suspend a transfer (Article 8(1), Article 12, Article 17(1) and Article 21 of Regulation (EU) 2023/1113)

Transfer of funds and crypto-assets

40. The risk-based policies for determining whether to reject, suspend or execute a transfer in accordance with Article 8(1), Article 12, Article 17(1) and Article 21 should consider the ML/TF risk associated with that transfer before deciding on the appropriate course of action.

41. 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 (see Section 5.3).

6.2. Rejecting or returning a transfer (Article 8(1) point (a), Article 12 point (a), Article 17(1) point (a) and Article 21(1) point (a) of Regulation (EU) 2023/1113)

Transfer of funds and crypto-assets

42. Where an IPSP, payee's PSP, ICASP or beneficiary's CASP decides to reject a transfer or when 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 had been rejected or returned because of missing information.

6.3. Requesting required information (Article 8(1) point (b), Article 12(1) point (b), Article 17(1) point (b) and Article 21 (1) point (b) of Regulation (EU) 2023/1113)

Transfer of funds and crypto-assets

43. Where the PSP, IPSP, CASP or ICASP request required information, the PSP, CASP, IPSP and CASP 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. Longer deadlines 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.

These deadlines should not exceed five working days in total.

44. 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 that the transfer has been suspended due to missing or incomplete information, as applicable.

Transfer of funds

45. Should the requested information not be forthcoming, as part of actions to be taken under Articles 8 and 12 of Regulation (EU) 2023/1113, PSP or IPSP should send a reminder to the prior PSP or IPSP in the transfer chain. As part of this, a PSP or IPSP should advise the prior PSP or IPSP in the transfer chain that, if the required information is not received before a particular deadline, the PSP or IPSP will reject the transfer and may treat the PSP or IPSP as repeatedly failing, as set out in article 8(2) and article 12(2). The PSP or IPSP should consider whether to subject the prior PSP or IPSP to internal risk monitoring.

46. Where the requested information is not provided by the set deadline, the PSP or IPSP , in line with its risk-based policies and procedures, as part of the actions taken under Articles 8 or 12 should:

    a. decide whether to reject or execute the transfer;

    b. 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 restrict or terminate its business relationship with that PSP or IPSP.

Transfer of crypto-assets

47. Should the requested information not be forthcoming, as part of actions to be taken under Articles 17 and 21, CASPs or ICASPs should consider sending a reminder to the prior CASP or ICASP in the transfer chain. As part of this, a CASP or ICASP should consider advising the prior CASP or ICASP in the transfer chain that, if the required information is not received before a particular deadline, the CASP or ICASP will reject the transfer or return the transferred crypto-

assets. The CASP or ICASP should consider whether to subject the prior CASP or ICASP to internal risk monitoring.

48. Where the requested information is not provided by the set deadline, the CASP or ICASP , in line with its risk-based policies and procedures, as part of the actions taken under Articles 17 or 21 should:

    a. decide whether to reject or return the transferred crypto-assets to the originator's crypto-assets account, previous CASP or ICASP in the transfer chain, or execute the transfer; or

    b. 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 restrict or terminate its business relationship with it.

6.4. Executing a transfer (Article 8(1), Article 12, Article 17(1) and Article 21 of Regulation (EU) 2023/1113)

Transfer of funds and crypto-assets

49. 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, based on all relevant risks, and provided that the condition in paragraph 50 is not met, 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.

50. 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.

6.5. Detecting missing or incomplete information after executing a transfer (Article 8(1), Article 12, Article 17(1) and Article 21 of Regulation (EU) 2023/1113)

Transfer of funds

51. Where a PSP or IPSP executes the transfer and 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.

Transfer of crypto-assets

52. 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.

Transfer of funds and crypto-assets

53. Where the requested information is not forthcoming within the timeframe set by the PSP, IPSP, CASP or ICASP, the PSP, IPSP, CASP or ICASP should, in line with its risk-based policies and procedures and in addition to rejecting or returning the transfer, consider the future treatment of the prior PSP, IPSP, CASP, ICASP or self-hosted address in the transfer chain for AML/CFT compliance purposes.

6.6. Contacting the prior PSP, IPSP, CASP and ICASP in the transfer chain (Article 8(1), Article 12, Article 17(1) and Article 21(1) of Regulation (EU) 2023/1113)

Transfer of funds and crypto-assets

54. 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 13, secure methods of contact in line with the provisions and obligations of Regulation (EU) 2016/679.

Transfer of crypto-assets

55. 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.

7. Repeatedly failing PSPs, CAPSs, IPSP or ICASPs (Article 8 (2), Article 12 (2), Article 17 (2), and Article 21 of Regulation (EU) 2023/1113)

7.1. Treatment of repeatedly failing PSPs, CAPSs, IPSP or ICASPs (Article 8(2), Article 12(2), Article 17(2), and Article 21 of Regulation (EU) 2023/1113)

Transfer of funds and crypto-assets

56. For the purposes of assessing repeated failures, PSPs and CASPs should at least include the following in their policies and procedures:

    a. a process to document all transfers with missing or incomplete information;

    b. a combination of quantitative and qualitative criteria to be considered when deciding whether to treat a PSP, IPSP, CASP or ICASP as 'repeatedly failing'.

57. Quantitative criteria referred to in paragraph 56 point (b) 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.

58. Qualitative criteria for assessing whether or not a PSP, IPSP, CASP or ICASP is repeatedly failing should at least include:

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.

59. Where the PSP or CASP decides to take steps before proceeding to a rejection, restriction or termination in accordance with Articles 8(2) point (a) of Regulation (EU) 2023/1113, the following order of steps should be applied:

a. PSPs and CASP should first consider the issuance of a warning in accordance with Article 8(2), Article 12(2), Article 17(2), and Article 21. That warning 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 and, where applicable, issue a further warning to the prior PSP, IPSP, CASP or ICASP in the transfer chain that any future transfers will be rejected.

b. the next step should be an assessment of the qualitative and quantitative criteria;

c. the final step should consist in rejecting any future transfers from that PSP, IPSP, CASP or ICASP or restrict or terminate the business relationship with the failing PSP, IPSP, CASP or ICASP.

60. 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.

7.2. Reporting repeatedly failing PSPs, CAPSs, IPSP or ICASPs to the competent authority (Article 8(2), Article 12(2), Article 17(2), and Article 21 of Regulation (EU) 2023/1113)

Transfer of funds and crypto-assets

61. PSPs, IPSPs, CASPs, and ICASPs should report to the competent authority referred to in Article 8(2), Article 12(2), Article 17(2), and Article 21 without undue delay, and no later than three months after identifying the repeatedly failing PSP, IPSP, CASP or ICASP.

62. The report should include the 'repeatedly failing' counterparty and the nature of the breach. 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.

63. Once a PSP, IPSP, CASP or ICASP identifies another PSP, IPSP, CASP or ICASP as 'repeatedly failing' to provide the required information, a notification to the authorities 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.

8. Transfers of crypto-assets made from or to self-hosted addresses (Article 14 (5) and Article 16 (2) of Regulation (EU) 2023/1113)

8.1. Individually identify transfers from or to self-hosted addresses (Article 14 (5) and Article 16 (2) of Regulation (EU) 2023/1113)

Transfer of crypto-assets

64. 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.

8.2. Transfers of crypto-assets made from or to self-hosted addresses (Article 14 (5) and Article 16 (2) of Regulation (EU) 2023/1113)

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

Transfer of crypto-assets

65. For the purposes of article 14(5) and Article 16(2), to determine whether the beneficiary or originator is using a CASP or a self-hosted address, the originator's CASP and the beneficiary CASP should rely on available technical means including but not limited to blockchain analytics,

third-party data providers, identifiers used by messaging systems. Alternatively, if such information cannot be retrieved via technical means, directly obtaining that information from the CASPs' customer.

66. The assessment should be done by the originator's CASP before the transfer is executed and the information transmitted in accordance with Article 14(5) of Regulation (EU) 2023/1113 or by the beneficiary CASP before the crypto-assets are made available to the beneficiary in accordance with Article 16(2) of that Regulation.

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

Transfer of crypto-assets

67. Where the crypto-asset transfer is not made from or to another CASP or any other obliged entity, but from or to a self-hosted address, in order to obtain the required information on the originator or beneficiary, the beneficiary's CASP and originator's CASP respectively, should collect the information from their customer. The beneficiary's CASP and originator's CASP should use suitable technical means to cross-match data, including blockchain analytics and third-party data providers, for the purpose of identifying or verifying the identity of the originator or the beneficiary.

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

Transfer of crypto-assets

68. For the purpose of assessing whether the self-hosted address in transfers above 1 000 EUR is owned or controlled by the CASP's customer, as referred to in Article 14(5) and Article 16(2) of Regulation (EU) 2023/1113, 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.

69. Where the amount of a transfer from or to a self-hosted address exceeds 1 000 EUR, the originator's CASP and beneficiary's CASP should verify whether the self-hosted address is owned or controlled by the originator and beneficiary, respectively, by using suitable technical means, which include at least two of the following:

    a. advanced analytical tools;

    b. unattended verifications as specified in the ''Guidelines on the use of Remote Customer Onboarding Solutions under Article 13(1) of Directive (EU) 2015/849''[15] displaying the address;

[15] EBA/GL/2022/15

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

d. 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;

e. signing of a specific message in the account and wallet software, which can be done through the key associated with the transfer;

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

g. 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.

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

a. the technical capabilities of the self-hosted address; and

b. the robustness of the assessment each method can deliver.

71. Where two methods on their own are not sufficiently reliable to ascertain the ownership or controllership of a self-hosted address, the CASP should ensure that a combination of more methods is used.

72. Where the self-hosted address is owned or controlled by a third person instead of the CASP customer, the CASP should, in addition to applying the verification requirement in accordance with Article 14 (5) or Article 16 (2) of Regulation (EU) 2023/1113, apply mitigating measures commensurate with the risks identified as per Article 19a of Directive (EU) 2015/849[16]. Verification in this context is deemed to have taken place when the CASP collects additional data from other sources to verify the submitted information, namely from:

a. blockchain analytic data;

b. third-party data;

c. recognised authorities' data; or

d. publicly available information, as long as those are reliable and independent.

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

Transfer of crypto-assets

[16] This provision will be introduced into Directive (EU) 2015/849 with the amendments to that Directive put in place in Regulation (EU) 2023/1113 and which will be applicable as of 30 December 2024.

73. CASPs should assess the risk associated with transfers from or to a self-hosted address as set out in Section 5.3 of these Guidelines and in accordance with the "The EBA's ML/TF Risk Factors Guidelines", using all information related to originators and beneficiaries, patterns, geographies, and information from regulators, law enforcement, and third parties.

74. CASPs should apply enhanced due diligence measures to transfers involving self-hosted addresses which present a high risk of ML/TF, in accordance with "The EBA's ML/TF Risk Factors Guidelines". Where such transfers raise suspicions of ML/TF, CASPs should report to the FIU in accordance with Directive (EU) 2015/849.

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

Transfer of funds

75. Where a transfer of funds is a direct debit, the PSP of the payee should send the required information on the payee to the PSP of the payer at the time when the direct debit mandate is established or modified. Upon receipt of that 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.

76. For the purpose of paragraph 75:

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

    b. verification in Article 4(4) of Regulation (EU) 2023/1113 should be carried out by the PSP of the payee 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 PSP of the payer (debtor PSP);

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

77. Where the PSP of the payer becomes aware, when receiving the direct debit collections, that the information referred to in Articles 4, 5 and 6 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), the options set out in Article 8(1) second subparagraph should be applied by the PSP of the payer. The PSP of the payer might choose to ask for the required information on the payer and the payee before or after debiting the payer's account, on a risk-based approach, to assess if the payment can still be

credited with missing information or the funds made available to the payee relying on information obtained from the payer and verified as part of the customer due diligence process, according to Section 4.

78. The PSP of the payer should leverage available communication channels to engage with the repeatedly failing payee's PSP prior to taking further actions to restrict or reject payments.

79. Policies and procedures should take into consideration possible changes to information across time, including name and address.

5. Accompanying documents

5.1. Draft 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" ('the joint fund 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 and PSPs and crypto-assets 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 fund transfer Guidelines and developed this consultation paper on the measures payment service providers (PSPs) and crypto-assets service providers (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 ('the 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 fund transfer Guidelines are repealed, this IA is performed on the entire draft 'Travel Rule Guidelines' and not just on the modifications resulting from the Regulation (EU) 2023/1113[17]. 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.[18] This is also important for crypto-asset transfers, given that those are also subject to similar money laundering and terrorist financing (ML/TF) risks as fund transfers. This was taken into consideration in the EU's 2020 'Action plan for a comprehensive Union policy on preventing ML/TF'[19] and in the 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 interpret and apply these Regulations inconsistently, leaving the Union's financial market exposed to the risk of ML/TF.

B. Policy objectives

Through these draft '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 draft '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.

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

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

[19] 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'[20]. 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 remained 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 fund transfer Guidelines', as mandated by Regulation (EU) 2015/847[21]. 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 draft '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 regards to the transfer of funds related points, the EBA did not aim to change the substance of requirements set by the 'Joint fund 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[22]. Specifically with regards 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.

[20] 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

[21] As mentioned previously, as the joint fund transfer Guidelines are repealed, this IA is done on the entire draft '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 fund transfer Guidelines.

[22] 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 to 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 their mandate.

Approach

Draft 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/ICAPs 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 on 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 draft 'Travel Rule Guidelines' allow PSPs/IPSPs to build on systems established under the 2017 'Joint fund 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/ISPSs and CASPs/ICASPs include the determination of the transfer of goods and services (Article 2(3)(a) and 5(b) of Regulation (UE) 2013/1113) and determining whether a transfer between PSPs, their agents or branches made for their own account are not subject to the Regulation 2023/1113 (Article 2(2) of Regulation (UE) 2013/1113). Furthermore, to provide guidance on the assessment and reporting by PSPs, IPSPs, CASPs and ICASPs (Articles 9, 13, 18 and 22 of Regulation (UE) 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 of the originators' CASPs, as required by the mandate (Article 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 than under 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 Options 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 assures 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. Further, due to the dynamic and fast-paced evolvement of PSPs and CASPs' business models, it would be at risk of the draft 'Travel Rule Guidelines' becoming outdated in the near future, due to the level of granularity it 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 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 can be complex and requires supervisors to have access to experts able to exert 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 they are conducive to a common approach in those areas where consistency and regulatory certainty is 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.

5.2. Overview of questions for consultation

Question 1. Do you agree with the proposed provisions? If you do not agree, please explain how you think these provisions should be amended, and set out why they should be amended. Please provide evidence of the impact these provisions would have if they were maintained as drafted'?