FIAU Financial Intelligence Analysis Unit

NOTICE TO SUBJECT PERSONS CARRYING OUT RELEVANT FINANCIAL BUSINESS INVOLVING THE TRANSFER OF FUNDS OR CRYPTO ASSETS FALLING WITHIN SCOPE OF THE TRANSFER OF FUNDS (RECAST) REGULATION.

On 9 June 2023, the Transfer of Funds (Recast) Regulation (TFR recast)[1] was published in the Official Journal of the European Union. The TFR recast extends the obligation to include information about the originator and beneficiary to a transfer of crypto assets, thereby aligning the EU's AML/CFT framework with the FATF's revised Recommendation 15 (the 'Travel Rule'). As of 30 December 2024, The TFR recast becomes applicable by repealing the Transfer of Funds Regulation.[2]

On 4 July 2024, the European Banking Authority (EBA) issued corresponding Guidelines which also become applicable as of 30 December 2024. The Guidelines aim is to provide detail on how certain provisions of the TFR recast are to be complied with by payment service providers (PSPs), intermediary PSPs (IPSPs), crypto-asset service providers (CASPs) and intermediary CASPs (ICASPs).

The Guidelines include detail on:

- The necessary information that must accompany a transfer of funds or crypto-assets.
- The steps that PSPs, IPSPs, CASPs and ICASPs should take to identify missing or incomplete information and subsequent action to be taken if the required information is missing or incomplete.
- How the information is to be transmitted and the characteristics of the systems to be used to transmit the information.
- The technical aspects of the application of the TFR recast vis-à-vis direct debits.
- The measures, including the criteria and means for identification and verification of identity of the originator or beneficiary of a transfer made to or from a self-hosted address.

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

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

Subject persons involved in a transfer of funds or crypto-assets are hereby being informed that with effect from 30 December 2024, the FIAU is adopting the EBA Guidelines as its own guidance in terms of Regulation 17 of the Prevention of Money Laundering and Funding of Terrorism Regulations (PMLFTR). With effect from this date, these Guidelines will become legally binding and will repeal and replace the FIAU "Guidance Note on transfers of funds having missing or incomplete information" issued on 25 October 2018.

When it comes to transfers of crypto-assets, the term CASP includes anyone who may be authorised as such in terms of the Markets in Crypto-Assets Regulation (MiCAR)[3] as well as anyone licensed in terms of the Virtual Financial Assets Act as a Virtual Asset Service Provider (VASP) and that, as at 30 December 2024, is benefitting from the transitory period allowed for the granting of authorisation under the MiCAR. In both instances, the Guidelines will find application whenever any such service provider will carry out a transfer of crypto-assets as defined in the TFR recast.

It should be noted that whenever a PSP, IPSP, CASP or ICASP identifies another PSP, IPSP, CASP or ICASP that repeatedly fails to provide the required information, a notification must be sent to the FIAU without undue delay and no later than three (3) months after identifying the repeated failure. The notification must be sent at compliance@fiaumalta.org in the form set out in Annex I to this Notice.

Subject persons are reminded that failure to comply with the requirements found in the TFR recast and the EBA Guidelines can result in enforcement action by the FIAU. These requirements are without prejudice to any other obligation that they are subject to in terms of the Prevention of Money Laundering Act (PMLA), PMLFTR, Implementing Procedures (IPs) and any other guidance issued by the FIAU from time to time.

[3] Regulation (EU) 2023/1114 of the European Parliament and of the Council of 31 May 2023 on markets in crypto-assets, and amending Regulations (EU) No 1093/2010 and (EU) No 1095/2010 and Directives 2013/36/EU and (EU) 2019/1937.

ANNEX I – NOTIFICATION TEMPLATE

Notification pursuant to Articles 8(2), 12(2), 17(2) and 21(2) of Regulation 2023/1113 (TFR recast)	
Name of reporting PSP/IPSP/CASP/ICASP	
Address of reporting PSP/IPSP/CASP/ICASP	
Date	
Name of repeatedly failing PSP/IPSP/CASP/ICASP	
Name of country in which the repeatedly failing PSP/IPSP/CASP/ICASP is authorised	
Short description of the nature of the breach, including: • **the frequency of transfers with missing information** • **the period of time during which the breaches were identified; and** • **reasons given by the repeatedly failing entity, if any, to justify the breach.**	
Short summary of the steps that the reporting PSP/IPSP/CASP/ICASP has taken.	

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.