Adan's response to EBA's consultation on preventing the abuse of funds and certain crypto-assets transfers for money laundering and terrorist financing purposes under Regulation (EU) 2023/1113

Adan's response

Introduction

Adan brings together more than 200 professionals in France and Europe - new players and established companies - who develop innovation and use cases for the decentralized web in all areas of the economy on a daily basis. By removing the obstacles to their growth and competitiveness, Adan is working towards the emergence and influence of French and European champions in the service of our digital sovereignty.

Adan promotes an appropriate, proportionate and catalytic framework for innovation, as well as a better understanding of new blockchain and Web3 technologies and their opportunities. Adan is thankful to the European Banking Authority (EBA) for allowing industry stakeholders to voice their opinions through this consultation on the draft guidelines regarding the travel rule within the framework of Regulation (EU) 2023/1113. The aim of the Association is to contribute to creating the most favourable environment possible in the EU for the development of a globally competitive digital asset industry.

Overall, Adan endorses the guidelines proposed by the EBA. These guidelines are set to supersede the previous Transfer of Funds Regulation (TFR) guidelines in light of the updated TFR, which now incorporates the Financial Action Task Force (FATF) travel rule for crypto-assets into EU legislation, effective at the end of next year. The guidelines detail the protocols for payment service providers (PSPs) and crypto-asset service providers (CASPs), including intermediaries, to identify and manage fund and crypto-asset transfers lacking complete information. Specifically, they provide directives for PSPs, CASPs, and the relevant national competent authorities (NCAs) on identifying factors, mitigating measures for money laundering/terrorist financing (ML/TF) risks, including scenarios involving self-hosted wallets, and nuances related to direct debits.

While certain areas may benefit from additional elaboration and clarification, neither the Association nor its members have pinpointed any significant concerns that could potentially obstruct the progression of the digital asset sector.

Adan remains wholly committed to assisting the EBA with any further information needed, pertaining either to the ongoing consultation or to future discussions anticipated to prompt additional consultations in the near term.

Adan's Response

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

1. General Provisions

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

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)

Question 1. Do you agree with the proposed provisions? If not, how should they be amended and why?

Adan agrees with the proposed provisions. Such Regulation should not apply to such transfer of funds or electronic money which are covered by other european laws.

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)

Question 2. Do you agree with the proposed provisions? If not, how should they be amended and why? Which regulatory choice would you prefer? What is the potential impact of the proposed provisions?

Adan agrees with the proposed provisions, but they should be supplemented. In particular, the Regulation also should set out what does not constitute a linked transfer, in order to clarify the concept. This would help to avoid ambiguity and ensure that the provisions are interpreted and applied consistently. In addition, it might make sense to include specific examples of what is considered a linked transfer, to provide clear guidelines for the entities concerned. This would reinforce understanding of the Regulation and ensure more effective and uniform application.

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

3.1. Messaging systems

Question 3. Do you agree with the proposed provisions? If not, how should they be amended and why? Which regulatory choice would you prefer? What is the potential impact of the proposed provisions? Explain.

In point **3.1.11**, 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.

The primary mission of protocols or messaging systems is to support regulatory compliant travel rule messaging, in an immediate and secure manner. While interoperability between travel rule solutions (protocols or messaging systems) is an ideal objective, it is not necessary in all cases.

- For example, a CASP may choose to adopt two different solutions to connect to the different groups of counterparties (*e.g.* one for regulated CASPs, another for unregulated entities for enhanced risk mitigation). In such a case, it is unnecessary to require a system to be able to convert information into the format of another system when that other system is not being used for a particular transmission. The current draft could be misinterpreted to mandate interoperability as a prerequisite for a Travel Rule solution, and it may have the unintended consequence of significantly reducing the available options for CASPs. Hence, we suggest revising the draft to avoid such unintended misunderstanding.

Based on Adan members' experience, to achieve the FATF's objective towards ensuring that the travel rule messaging is transmitted immediately and securely, maintaining data protection is the key challenge in any interoperability discussion. To support an end-to-end encrypted transmission, a public key needs to be securely transmitted from a data controller (*e.g.* beneficiary's CASP) to another data controller (*e.g.* originator's CASP), ideally for each transmission. In most of the cases and if the Draft 11 proposal becomes mandated, it would entail that the conversion of data format will require the access to naked data. For this reason, it is ideal to process this conversion within the system of the data controller (e.g. CASP) rather than by a third party. If the guidelines suggest "to ensure that their systems are able to convert information into a different format", it could be misread as to enable a messaging system, which could be a third party, to be able to access naked (unencrypted) personal data of the customers. For this reason, Adan strongly suggests to the EBA to emphasise the importance of data protection obligation, when personal data traverses across multiple protocols or messaging systems. strongly suggest to emphasise the importance of data protection obligation, when personal data traverses across multiple protocols or messaging systems.

Where PSPs, IPSPs, CASPs and ICASPs use multiple protocols or messaging systems for a transmission or reception of information, they should ensure that the protocols or systems are able to support transmission or reception of information without error or omission, in an immediate and secure manner.

In point **3.1.12**, we would also like to highlight the fact that 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"*. The EBA Guidelines on ICT and security risk management provide a comprehensive framework for general ICT and security

management for financial institutions. Where using third party systems, particular attention must be paid to Article 3.2.3. ("Use of third party providers") of the guidelines.

Given the nascent stage of travel rule adoption, there exist varying levels of maturity among Travel Rule protocols and messaging systems. This attracted a particular concern of the FATF, which was elaborated in the Targeted Update on Implementation of the FATF Standards on VAs and VASPs (June 2023) where the FATF recognised the issue of sub-standard Travel Rule protocols or messaging systems and detailed out requirements.

- ➔ In this context, **Adan suggests to clarify further by distinguishing the way messaging systems are being used within the broader IT systems and what is required in the context of outsourcing arrangements**. PSPs, IPSPs, CASPs and ICASPs should use systems for the transfer of information in a secure manner as set out in the "*EBA Guidelines on ICT and security risk management*", "*EBA Guidelines on outsourcing arrangements*" and, where applicable, Article 19 of Payments Services Directive.

In point **3.1.13** and 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.

Travel rule implementation is a complex exercise that has deep impact on the various critical systems of CASPs or ICASPs (*e.g.* counterparty relationship, user interface for information collection, DB structure, wallet operation, deposit and withdrawal of crypto-assets, internal or on-chain surveillance, personal data protection, etc.). Also, CASPs or ICASPs come in various sizes, unlike traditional financial institutions. Due to this, it is extremely difficult for CASPs or ICASPs to switch from one messaging system to another one.

On this basis, Adan agrees with the staged approach with the timeline of Regulation (EU) 2023/1113's enforcement. At the same time, we express our concern on the risk of CASPs or ICASPs being stuck with non-compliant messaging protocols or systems. The current draft may give rise to misinterpretation that non-compliant protocols systems are tolerated and non-compliant practices are accepted. For this reason, we suggest to ensure the technical limitations to be temporary and to hold the principle of timely and secure transmission to serve the intent of Regulation (EU) 2023/1113 and data protection.

- ➔ **Consequently, Adan suggests that, by way of derogation from paragraph 10 and until July 31, 2025, CASPs and ICASPs may exceptionally use infrastructures or services with technical limitations requiring additional or alternative policies and**

procedures to comply 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 temporary technical limitations, in a timely and secure manner.

- Adan acknowledges that a transitional adaptation period for entities to fully comply with TFR requirements has been already mentioned. However, achieving full compliance within the proposed timeframe appears challenging, if not impossible, given the current conditions for CAPS. It is understood that when a CAPS cannot maintain a completely optimal system, it implements additional procedures to offset these limitations. Yet, the introduction of such a regime might lead to confusion and misunderstandings among CAPS, creating a landscape filled with numerous difficult-to-reconcile situations in the future. Moreover, the current scenario remains immature across the board—be it from the regulator's perspective, the CAPS, or the service providers. Specifically, from the regulator's side, definitive guidelines for the concrete application of TFR are still pending publication, casting uncertainty over the regime's implementation. In the view of Adan, proposing to establish a regime by December 31, 2024, without a fully defined framework seems premature. Regarding service providers, only a handful appear to be fully operational in terms of functionality by the set deadline. A very limited number of service providers can offer an interoperable solution meeting TFR requirements. As they await further guidance, service providers are not yet in a position to deliver a complete product.

- Lastly, concerning CAPS, this stringent deadline might result in significant management challenges in selecting an appropriate solution. Hastily moving forward with these solutions could distort competition quickly and potentially lead to monopolistic outcomes. This rush could significantly increase costs for CASPs, who would find themselves pressed for time and without viable alternatives. Considering the extensive changes required for CAPS, allowing additional time to establish a fully operational system seems more prudent than enforcing a transitional period that appears difficult, if not impossible, to implement.

➔ **Given these considerations, Adan recommends extending the deadline to June 30, 2025, to ensure a more feasible and effective compliance environment for all stakeholders involved - and particularly for CASPs.**

In point **3.1.14,** 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.

With regards to point b. above, transmitting information immediately and securely, in the context of virtual asset (VA), the completion of VA transfer could mean **(i)** initiation of blockchain transaction, **(ii)** completion of required blockchain confirmations for transfer-out, **(iii)** completion of required blockchain confirmations for transfer-in, **(iv)** making the transferred-in VA available to user. Depending on the type of blockchain network and the policy of the CASP of the beneficiary, the gap between **(i)** ~ **(iv)** can vary from a few seconds to a few days. If the policy of the beneficiary CASP allows, virtual assets can be made available to the beneficiary at the moment of **(iii)** completion of required blockchain confirmations.

As clarified in the FATF Guidance on VA and VASP, Article 185, 'immediately' in the context of INR. 15, para 7(b) refers to submitting information prior to, simultaneously or concurrently with the VA transfer itself. Table 2.1. of the Targeted Update on Implementation of the FATF Standards on VAs and VASPs further clarifies the objective of immediate information sharing as preventing the VA transfers from being made available to illicit actors.

➔ **For this reason, it is necessary to submit the required information as soon as possible, but no later than the moment of the transfer itself (in the VA context, the initiation of blockchain transaction).**

In this context, we express our concern that the expression *'before the transfer is completed*' could lead to various misinterpretations, delaying further the moment of information submission. Hence, **Adan suggests aligning the information submission timing to be consistent with the FATF standard and we suggest rewording to transmit the required information immediately and securely, before or at the time of the virtual assets transfer.**

In point **3.1.15,** 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.

As Article 12 mandates assessment in the context of IT security and outsourcing arrangements where applicable, it is necessary to define key assessment areas in the context of Travel Rule and personal data protection within this article. Given that the purpose of the assessment is to ensure Regulation (EU) 2023/1113 and Regulation (EU) 2018/1725

or other applicable personal data regulations, we are of the opinion that the key requirements should continue to focus on regulatory compliance.

Regarding compliance requirements of messaging protocols, the FATF Targeted Update on Implementation of the FATF Standards on VAs and VASPs (June 2023) has detailed out common shortcomings. Table 2.1 of the targeted update shows various issues identified within available messaging protocols, requesting the protocols to make improvements and meet the FATF requirements. We are of the opinion that these issues are pressing problems, hindering successful Travel Rule compliance and an urgent remedy is needed given the very short timeline.

The FATF acknowledges that there has been limited progress in interoperability between Travel Rule compliance solutions limiting the capability of VASPs to send Travel Rule information. But at the same time, the FATF recognizes that interoperability is not a precondition of Travel Rule implementation.

We are of the opinion that while interoperability between messaging protocols is useful, Travel Rule and data protection regulatory compliance itself, should be placed as the higher priority. In this context, we suggest laying out key requirements on messaging protocols for regulatory compliance in Article 15.

Top priority is to ensure that the Travel Rule messaging protocol must be interoperable with the CASPs or ICASPs' necessary internal and external systems. Unlike traditional financial institutions, CASPs or ICASPs have a very wide spectrum in business size and nature. For this reason, the systems specific to a CASP that needs to be interoperable may differ greatly from another CASP. For example, if a CASP only conducts very limited business activity connected with a particular CASP, it may not even need to adopt a third party messaging protocol. So, we are of the opinion that a CASP or ICASP needs to identify the necessary systems it needs to be connected to and then secure the right messaging protocol fit for that purpose, rather than wait for a single messaging protocol connected with every system.

There is a perception that the lack of interoperability between messaging protocols leads to less counterparty relationships, hindering the adoption of Travel Rule. But in our field observation, the actual bottleneck in the expansion of counterparty relationships is the counterparty DD obligation exacerbated by slow adoption (or enforcement) of the VASP regulatory regime. Just like a bank is not connected with all the banks in the world directly, it is not possible nor desirable for a CASP or ICASP to be connected to all VASPs. Until the wider option of regulative regime eases the complication of counterparty DD, we expect there to be limited interoperability between VASPs with or without interoperability between messaging protocols.

Other than interoperability with necessary systems, we suggest addressing common issues found within messaging protocols. There still exists varying interpretations on what constitutes immediate and secure messaging. Verification on collected beneficiary or beneficiary's CASP is missing in many protocols, undermining the purpose of the

name-screening exercise. Article 16 paragraph 3 of Regulation (EU) 2013/1113 requires "before making the crypto-assets available to the beneficiary, the crypto-asset service provider of the beneficiary shall verify the accuracy of the information on the beneficiary". In practice, it is desirable for the originator's CASP to verify declared beneficiary information against the beneficiary's CASP prior to transferring crypto-assets. Some messaging protocols support only pre-defined crypto-assets, further limiting Travel Rule compliance capability, greatly. Lastly, the nature of blockchain transactions requests for highly available and scalable architecture to support timely messaging in a compliant manner.

Adan suggests, when choosing the messaging protocol that CASPs and ICASPs should ensure, that the protocol's architectures are sufficiently robust to enable the compliance with Regulation (EU) 2023/1113 and applicable data protection regulations by assessing the protocol's architecture for:

a. seamless communication with necessary systems of both within and outside of CASPs and ICASPs for the transmission and reception of required information or enhanced risk mitigation measures;

b. immediate and secure information transmission, before or at the time of the transfer;

c. counterparty verification;

d. support for all types of crypto-assets; and

e. availability and scalability of the protocol.

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

Question 4. Do you agree with the proposed provisions? If not, how should they be amended and why? Which regulatory choice would you prefer? What is the potential impact of the proposed provisions?

In point **5.3.34.d** and point **5.3.34.e,** 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. Transfers with entities based in a third country that does not have licensing regimes or does not regulate PSP/CASP activity, or with self-hosted addresses.

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

4.1. 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)

Question 5. Do you agree with the proposed provisions? If not, how should they be amended and why? Which regulatory choice would you prefer? What is the potential impact of the proposed provisions?

In point **6.3.43,** 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 **(i)** more than two parties in the transfer flow (including intermediaries and non-banks); and **(ii)** at least one PSP, IPSP, CASP or ICASP that is based outside of the EU.

➔ **Adan suggests that these deadlines should not exceed five working days in total.**

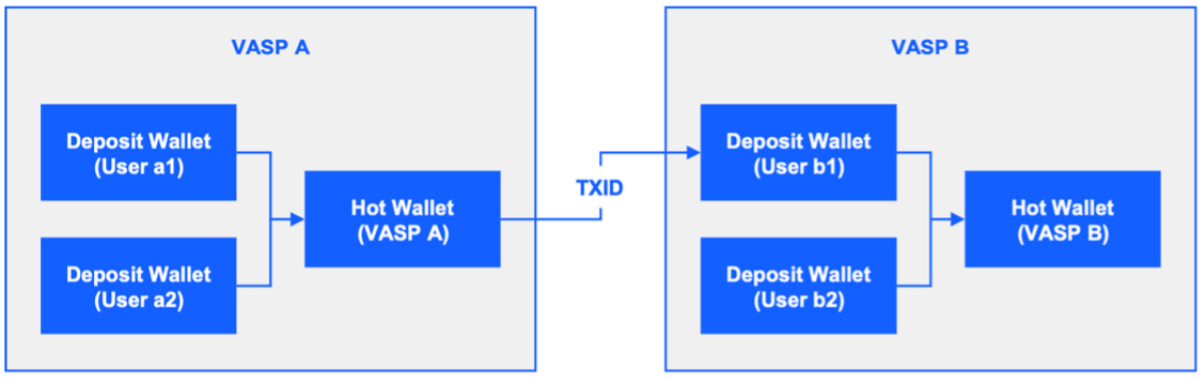
4.2. Contacting the prior PSP, IPSP, CASP and ICASP in the transfer chain (Article 8(1), Article 12, Article 17(1) and Article 21(1) of Regulation (EU) 2023/1113)

Question 6. Do you agree with the proposed provisions? If not, how should they be amended and why? Which regulatory choice would you prefer? What is the potential impact of the proposed provisions?

In cases where a transfer is not originating from a CASP or ICASP, it is not possible to inform the CASP or ICASP when returning a transfer. Also, it is not always possible nor desirable to return a transfer back to the originating CASP, ICASP, VASP or self-hosted wallets. So, we suggest limiting the obligation to inform only when the transfer is from a CASP or ICASP.

The FATF guidance or local regulations do not specifically prescribe requirements on travel rule non-compliance return policy. This leads to VASPs adopting various practices on return policies. Key considerations on a return policy are: **(a)** where to return to; **(b)** who to return to; **(c)**applicability of travel rule compliance.

Most VASPs operate aggregated wallets (usually, hot wallets) to process multiple users' withdrawal requests. While deposit wallet addresses are unique to each user, withdrawal wallet addresses ('from' addresses in blockchain transactions) are not. In case a VASP relies on a third-party custodian, a blockchain wallet which initiated a certain VA transfer may not even be managed by the particular VASP. For this reason, simply returning back to the 'from or originating address' identified by a blockchain explorer or scan may lead to the loss of the virtual asset. In case a VASP wishes to return the virtual assets back to the originator's account managed by the ordering VASP, it may need to separately collect the deposit address of the originator with the consent of both originator and intended beneficiary.



In case the originator is not the same person as the intended beneficiary, there is the complication of who to return the assets to: back to the originator or to a wallet address in the name of the intended beneficiary managed by another VASP (among the approved VASPs that has completed the counterparty DD).

This is an interconnected problem with iii) the applicability of travel rule on the return process. In case Travel Rule compliance needs to be applied to the return transaction, sending the transfer back to the originator may not be feasible since there is no guarantee that the originator - not a user of the VASP - has an account amongst the approved VASPs. If it is possible not to apply Travel Rule on the return process, then returning the transfer back to the originator is a possible option. But even in this case, there needs to be specific consent from both originator and intended beneficiary regarding the collection of data and return of assets. Name screening on originator and on-chain screening on requested destination wallet address (not 'from' address) will be necessary to avoid transferring assets to illicit actors. This transaction will generate a withdrawal transaction towards an 'out of approved VASP' and may need to pass sufficient internal approvals processes with written record.

Considering such complications, we are of the opinion that returning the asset transfers back to the intended beneficiary's other account kept in an approved VASP - upon the consent of the originator - within travel rule or an enhanced risk mitigation process is a more straightforward solution. Still, this practice runs the risk of abuse in the form of a chain of asset transfers, circumventing otherwise impossible transfers. For example, considering VASPs A, B, and C with counterparty relationships established only between VASP B and VASP C, the return policy can be abused to form a chain of transfer from VASP A then B then C, effectively allowing VASP A to indirectly transfer the assets to C. For this reason, the return can only be processed upon necessary considerations of relevant facts and internal approvals to discourage any abusive practice.

Lastly, if not required by regulation, a VASP needs to make the decision whether to apply the Travel Rule or an enhanced risk mitigation measure upon returning the transaction. We are of the opinion that the Travel Rule or an enhanced risk mitigation measure should be applied even in the case of a Travel Rule return transaction. As described in the section above, omitting Travel Rule does not make the return process any easier for a VASP or its user due

to the responsibility of name screening and on-chain monitoring accompanied by data collection complications. Also, in case a user has a (Travel Rule not-compliant) deposit, the user usually has an account in another VASP, making the return more feasible. In case a VASP wishes to further mitigate the risk associated with a return transaction, limiting the beneficiary only to the first party (the user itself) could be a straightforward option as long as it can secure consent from the originator upon the intended return transaction.

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 to originator's CASP or ICASP, instead of requesting the missing information, they should inform the recipient PSP, IPSP, CASP or ICASP in the transfer chain that the transfer had been rejected or returned because of missing information.

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

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

Question 7. Do you agree with the proposed provisions? If not, how should they be amended and why? Which regulatory choice would you prefer? What is the potential impact of the proposed provisions?

In point **8.2.3.69**, where the amount of a transfer from or to a self-hosted address exceeds 1000 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;

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.

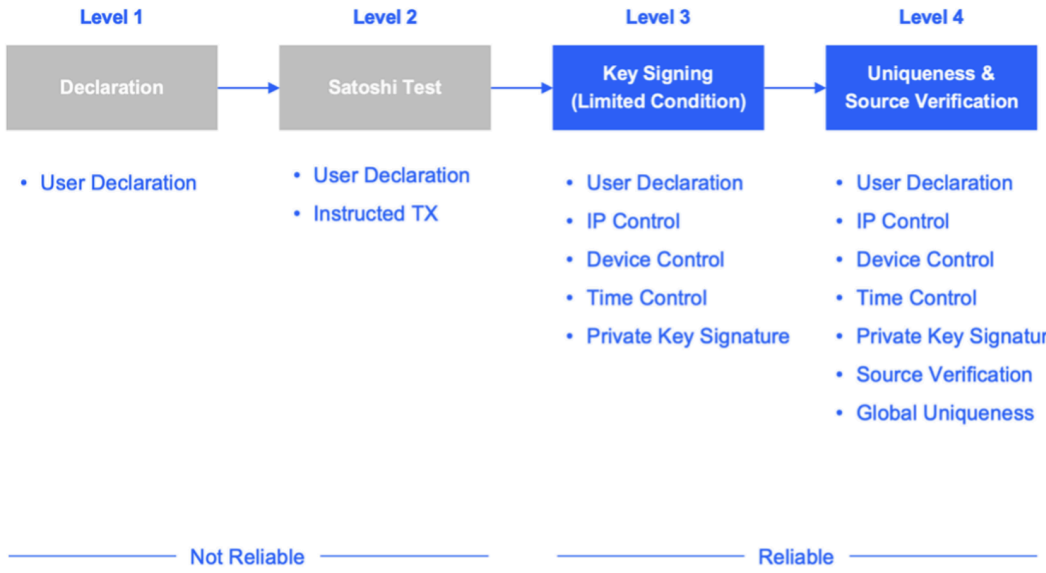
Just like banks facilitating cash deposits or withdrawals, transfers in and out from/to self-hosted wallets are unavoidable. When a user has a legitimate property right on a digital asset, it is very difficult to reject a withdrawal request to a self-hosted wallet owned by the user. A user may choose to use certain CASPs only for the purpose of exchange but not for the purpose of storing their asset. In such a case, forcing the user to use the custodian or storage service offered by the CASP or other CASPs is not appropriate. But unlike cash transactions happening in banking services, a transaction with a self-hosted wallet is not face-to-face. There exist various limitations on cash transactions or transportation (especially for cross-border), but blockchain transactions are borderless. Handing over a stack of cash is a relatively cumbersome exercise depending on the amount and travelling distance but sharing a private key of a certain self-hosted wallet is instant, borderless and hard to trace.

Conversely, a blockchain transaction involving a self-hosted wallet leaves an immutable, publicly available record. Unlike a wallet managed by a CASP, any withdrawal from a self-hosted wallet can be deemed to be made by the beneficial owner of the wallet. While cash transactions hardly leave any trace to construct the transaction back, a self-hosted wallet leaves a rich and dynamic dataset to be used for ML/TF risk mitigation.

A transaction with a self-hosted wallet can be seen as a trade-off problem between property right and ML/TF risk, requiring to strike an equitable balance. But given the nature of blockchain transactions, it is at its core, a data problem. More specifically, the question is how to obtain sufficient data for ML/TF risk mitigation to support a user's legitimate property right.

Whilst FATF specifies that self-hosted wallets are out of scope of the Travel Rule, the FATF guidance and subsequent updates highlight their inherent risks and suggest a variety of mitigation measures. Under this guidance, most of the local regulations mandate certain risk mitigation measures for self-hosted wallets. Some jurisdictions are restricting transfers to or from self-hosted wallets to first party transfers only.

However, establishing ownership (or control) of a self-hosted wallet can be challenging and there have been varying practices in the industry, which we summarise below.



Source: VerifyVASP Classification of Unhosted Wallet Verification Methods

a. **Level 1** — a simple declaration or digital signature from the user that they own the self-hosted wallet. This can be perceived as an ineffective control by most regulators.
b. **Level 2** — a manual test such as a Satoshi test that is a combination of user declaration coupled with a penny test of a specified amount to the self-hosted wallet. This method may not be reliable as a third party could simply transfer the required test amount. It is also manual and not scalable.
c. **Level 3** — involves user declaration and using the private key signature from within the VASP's own interface with the limitation of same time, IP address and device. At the moment, this is generally perceived as relatively reliable.
d. **Level 4** — is similar to Level 3 but further enhances risk mitigation with global uniqueness and source verification. Global uniqueness means there is only one beneficiary owner of a certain self-hosted wallet across multiple VASPs. Source verification traces deposit history of certain self-hosted wallets to verify how much deposit was actually from the beneficiary owner. Unlike Level 3 approach, this provides a dynamic dataset, updating the risk profile of certain self-hosted wallets in real-time.

➔ **Consequently, Adan suggests ensuring the ownership of self-hosted wallets to be on an on-going basis, not just one time. Also, we suggest reiterating the purpose of self-hosted wallet verification as i) proof of private key ownership and ii) prevention of false identity to give CASPs and ICASPs certain flexibility to adopt any suitable new technology available in the future.**

➔ **We also suggests the rewording** *"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 currently owned or controlled by the*

originator and beneficiary, respectively, by using suitable technical means for the purpose of verifying the access to the private key and preventing false identity, which include at least two of the following:"

In point **8.2.3.70,** 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.

Finally, in point **8.23.69**, Adan suggests amending this provision to reconsider the inclusion of method (a) and modifying (e) to include language on conducting this signing from within the CASP's interface for added reliability of the method.

- **Additional comments on Counterparty Due Diligence**

Adan also noted that the provisions are silent on the due diligence requirement on relationships between CASPs, or counterparty due diligence as required by paragraph 60 of Regulation (EU) 2013/1113 as pasted below.

> (60) Relationships established between crypto-asset service providers and entities established in third countries for the purpose of executing transfers of crypto-assets or the provision of similar crypto-asset services present similarities to correspondent banking relationships established with a third country's respondent institution. As those relationships are characterised by an ongoing and repetitive nature, they should be considered a type of correspondent relationship and be subject to specific enhanced due diligence measures similar in principle to those applied in the context of banking and financial services. In particular, crypto-asset service providers should, when establishing a new correspondent relationship with a respondent entity, apply specific enhanced due diligence measures in order to identify and assess the risk exposure of that respondent, based on its reputation, the quality of supervision and its anti-money laundering and counter-terrorist financing (AML/CFT) controls. Based on the information gathered, the correspondent crypto-asset service providers should implement appropriate risk mitigating measures, which should take into account in particular the potential higher risk of money laundering and terrorist financing posed by unregistered and unlicensed entities. That is especially relevant as long as the implementation of the FATF standards relating to crypto-assets at global level remains uneven, which poses additional risks and challenges. EBA should provide guidance on how crypto-asset service providers should conduct the enhanced due diligence and should specify the appropriate risk mitigating measures, including the minimum action to be taken, when interacting with unregistered or unlicensed entities which provide crypto-asset services.

This counterparty due diligence requirement has proven to be an effective tool and key component of travel rule compliance in other countries. In addition to mitigating the regulatory arbitrage arising from the nuances of travel rule regulations internationally, it also addresses many of the anticipated issues raised or implied in these provisions if transfers are limited to counterparties that have passed due diligence.