Revolut

Response to EBA Consultation Paper on the Travel Rule Guidelines[1]

Feb 2024

FOREWORD

Revolut is one of Europe's largest fintechs, with more than 25 million customers in Europe and over 40 million customers in other 40 markets around the world. Our medium term vision is to be the world's best global bank, servicing all the financial needs of consumers, businesses and merchants.

We offer a wide range of financial services and currently operate under a variety of licences depending on the jurisdiction. In the EU, we operate as a bank supervised by the Bank of Lithuania and the European Central Bank as a significant institution. We also provide crypto asset services for European users under the supervision of the Cyprus Securities and Exchange Commission, enabling buying and selling of a selection of some of the most mainstream crypto assets and also withdrawals and deposits of some of these assets via the blockchain. We also work closely with international standard-setting bodies by proving our input and participating in working groups.

We provide digital asset services, alongside our traditional payment, insurance and trading services, due to demand from our customers wanting to be able to access crypto assets from within our ecosystem. As we are aiming to be the main financial provider to our customers over their lifetime, we take a particularly controlled risk approach to crypto assets - both in terms of the exposure of our customers (who in general invest a very small portion of their total assets) and when it comes to key compliance process (e.g. AML, KYC, risk analysis). For example, unlike competitors, we do not allow access through our platform to 'privacy coins' or 'mixing services' which provide another route for bad actors to obfuscate the origin funds or true owners of crypto assets. We also are constantly looking for ways to help our customers be more informed and responsible in their approach to crypto.

We are happy to contribute to the EBA's work on an ongoing basis by providing our views on the launched consultations and participating in the industry working group. We would welcome the opportunity to discuss our views on the EBA's consultation in further detail with you.

[1] https://www.eba.europa.eu/sites/default/files/2023-11/cc8eb1e9-df10-4517-81a1-de4a8c9d0360/Consultation%20paper%20on%20draft%20travel%20rule%20Guidelines%20under%20Regulation%20%28EU%29%202023_1113.pdf

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

We appreciate the opportunity to contribute to the Guidelines on preventing the abuse of funds and certain crypto-assets transfers for money laundering and terrorist financing purposes under Regulation (EU) 2023/1113 (the Travel Rule Guidelines). Below are our detailed recommendations for paragraphs **69 and 71 of Section 8.2.3**.

Whilst it is clear that a lot of careful thought has been put into the details of guidelines 69 and 71, we believe that some small amendments to current drafting are required due to following:

1. In many cases, there will not be two viable methods for the verification of ownership of self hosted wallets (i.e. the methods currently listed in guideline 69 as drafted), especially for Unspent Transaction Output (UTXO) asset transfers such as Bitcoin
2. Some of the technical means of verification listed (69.e and 69.f) require significant technical expertise by customers, are not often supported by wallets, and introduce the risks of non-technical customers potentially losing funds
3. Guidelines 69 and 71 as drafted will hinder the EUs competitiveness as a jurisdiction due to points 1 and 2 without some drafting amendments, and also put EU based crypto asset service providers (CASPs) at a disadvantage to CASPs in other jurisdictions such as the UK which has approached self hosted wallet regulation differently

With some minor alterations however, we believe that guidelines 69 and 71 can achieve each of the following goals:

- Effective mitigation of FinCrime risks associated with self hosted wallet transfers
- Good customer experience and avoidance of customer harm
- EU competitiveness

Why should they be amended?

1. In many cases, there will not be two viable methods for the verification of ownership of self hosted wallets (i.e. the methods currently listed in guideline 69 as drafted), especially for UTXO asset transfers such as Bitcoin

The means of verification identified in 69.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;”)* is also commonly referred to as a Satoshi Test.

Unfortunately due to the way that all UTXO assets work (including Bitcoin, Litecoin and Bitcoin Cash etc) the vast majority of Satoshi Test verification attempts will fail for reasons which we describe below. And since Bitcoin is still the most popular crypto asset by far with a market dominance of 52% (as of 18th Feb 2024)[2], this is clearly an issue.

Additionally, due to the fact that the complexity of a UTXO transaction is not understood by most users and is abstracted away from them by all wallets, legitimate customers will not understand why their attempted Satoshi Tests fail. They will thus be prevented from moving their money to or from legitimate sources or destinations. This problem is already occurring in jurisdictions such as Singapore which have a mandated Satoshi Test requirement, as evidenced by many complaints from customers in public forums such as Reddit who find their Bitcoin trapped on centralised Singaporean platforms due to repeated failure of Satoshi Tests. Anecdotally, this is having an impact on Singapore's competitiveness as a jurisdiction in the space as it is competing with jurisdictions such as the UK which have followed a different yet effective approach regarding mitigating self hosted wallet risk.

In order to understand the problems of using Satoshi Tests as a means of verification it is first necessary to review how UTXO assets such as Bitcoin actually work. UTXO stands for Unspent Transaction Output. Unlike an account to account based transfer like a traditional bank transfer (which essentially has a sending account number, a receiving account number and a value), UTXO transactions work very differently under the hood:

Imagine a user, Alice, with an empty Bitcoin Wallet. Alice wants to receive Bitcoin from her friend Bob and so opens her Bitcoin wallet and clicks the "Deposit" button. Alice's Bitcoin wallet will generate a Bitcoin address that she can share with Bob in order that Bob can send her funds which will be received at this address. We shall call Alice's address Address 1. Alice shares Address 1 with Bob, and Bob sends Alice $5 worth of Bitcoin. Alice's wallet now has $5 worth of Bitcoin as balance. The $5 represents the Output of the Transaction that Bob created to send these funds to Alice. This Output is Unspent because Alice has not yet herself spent this $5. And most importantly, this $5 UTXO is essentially sitting on Address 1 of Alice's wallet.

Alice also wants to receive Bitcoin from her friend Chen so she again opens her Bitcoin wallet and clicks the "Deposit" button. Alice's wallet again displays an address to allow her to receive Bitcoin from Chen, but the address displayed is not Address 1, it is actually a brand new address that we shall call Address 2. *Bitcoin wallet/address relationships are not 1:1 like user bank account/IBAN relationships. Most wallets generate a new address for every single new deposit*. *In addition to that, Bitcoin wallets also generate new addresses for 'Change' when sending funds, which further adds to the complexity of the situation (we shall explain 'Change' shortly)*. Alice probably won't even be aware that the address (Address 1) she shared with Bob is different to the address (Address 2) she has just shared with Chen. Chen then sends Alice $15 to Address 2. As before this $15 represents the Output of the Transaction that Chen created to send funds to Alice, and it is Unspent because Alice has not yet spent this $15. Alice's wallet just now displays her total Bitcoin balance as $20. The fact that $5 is sitting as a UTXO on Address 1 and $15 is sitting as a UTXO on Address 2 is not revealed to Alice by her wallet, is not understood by the vast majority of crypto users, and Alice has no control over it. This is not dissimilar to the fact that most people don't

[2] CoinMaketCap: Bitcoin Dominance

understand the technical details of how SWIFT or BACS transfers actually work under the hood, but don’t actually need to in order to use them.

Alice decides she wants to withdraw some Bitcoin from her CASP account to the Bitcoin wallet where she has received funds from Bob and Chen. In order to do that Alice needs to add her wallet as a beneficiary in her CASP. Alice opens her wallet and clicks the “Deposit” button to get her wallet address. As before her wallet generates a brand new wallet address that we shall call Address 3. As her CASP is in a jurisdiction that has mandated the Satoshi Test in order to verify self hosted wallet ownership, her CASP asks her to send a small amount of funds from Address 3 as per Satoshi Test requirements to verify wallet ownership. From the CASPs point of view, this address represents her wallet, which isn’t in fact accurate for the reasons described above i.e. there is not a 1:1 relationship between wallets and addresses for UTXO assets, and users cannot control the underlying mechanisms of address or UTXO management because it is extremely complex. Alice opens her Wallet, sees her balance of $20, and sends $1 from her Wallet to her CASP as instructed. What actually happens now under the hood is very different to a traditional finance transfer and clearly illustrates why the Satoshi Test will fail in most cases for UTXO assets:

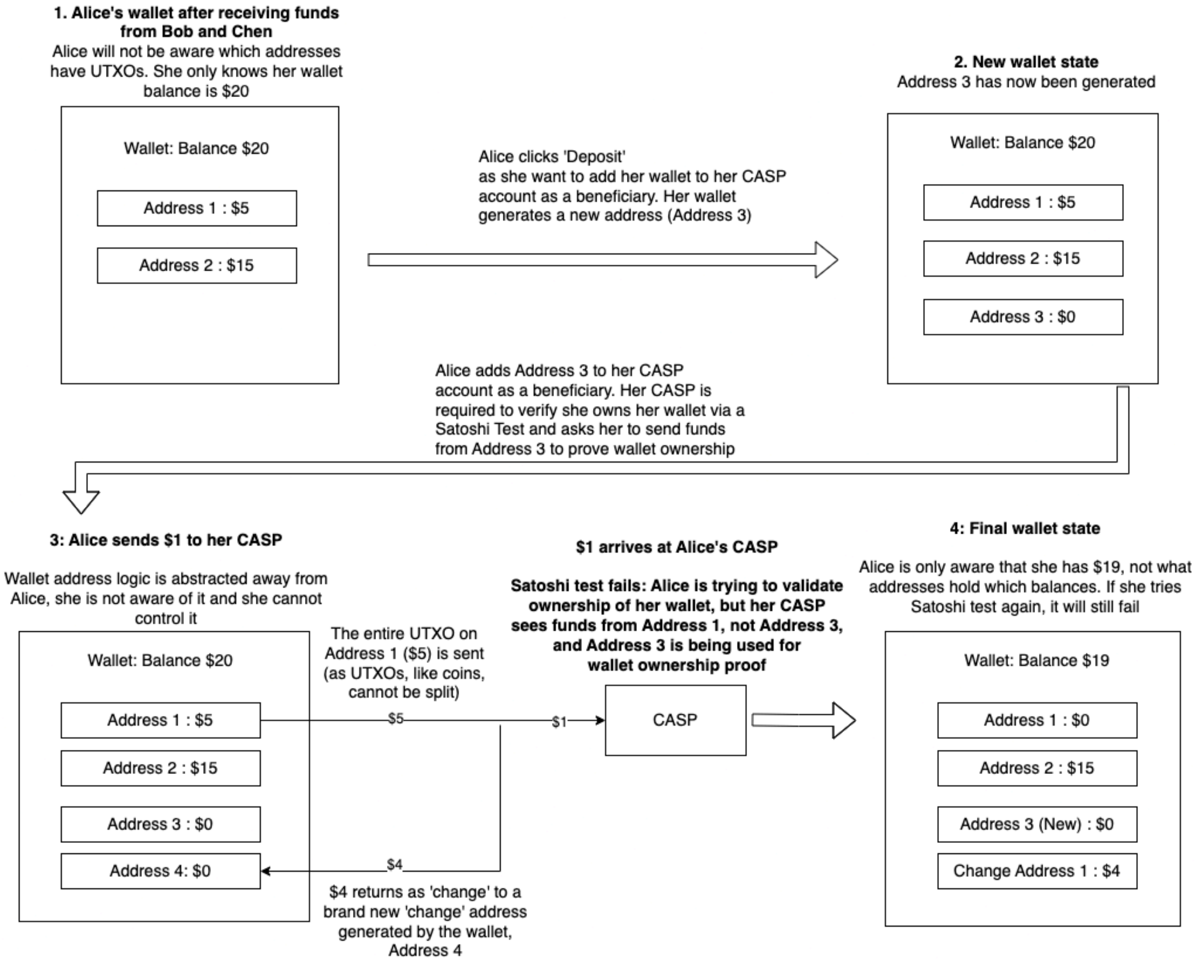
UTXO assets work by constructing new transactions with Inputs that are previous transaction UTXOs in order to transfer value. At this point it is helpful to think of UTXOs as traditional coins in a wallet in someone's pocket. These coins are in this wallet as a result of previous transactions (so essentially they are UTXOs as per our definition). In a traditional transaction with coins, you cannot split individual coins, you have to pay with whole coins, and potentially receive change in return where you cannot create the exact payment amount required with the coins you have. The same is true for UTXOs: you can’t use a part of a UTXO in a transaction, you have to use the whole thing. And this means that just like paying with traditional coins, you will then receive change in cases where the value of the UTXO you paid with is larger than the amount required for the transaction. In our example, Alice’s wallet assesses Alice’s current UTXOs in order to decide which one to use as an input to this transaction (i.e. the transaction to send $1 to her CASP account). Alice currently has two UTXOs in her wallet, $5 and $15. Alice’s wallet decides to use the smaller of the two UTXOs and since UTXOs are like coins and cannot be split, the entire $5 is used as an Input to this Transaction. As Alice only wants to send $1 to her CASP account, but this transaction has an input of $5, just as if Alice was paying with coins, she must receive $4 of change in order for the Output of the Transaction to match her intention. Her Wallet handles this automatically under the hood and constructs a transaction that has the following structure:

- **Input**: $5 (UTXO from Bob’s previous transaction sitting on Address 1)
- **UXTO i**: $1 (sent to Alice’s CASP account)
- **UTXO ii**: $4 (sent to a newly generated address in Alice’s wallet, generated on the fly by her wallet in order to receive the ‘Change’ from this transaction. We shall call this address Address 4)

Alice’s wallet now has completely spent her original UTXO of $5 so there is no longer a UTXO sitting on Address 1. Alice’s wallet still has her second UTXO of $15 sitting on Address 2, and now has a new UTXO (the change from this latest transaction) of $4 sitting on Address 4. Alice will not be aware of all this complexity going on under the hood. From her perspective, she has just sent $1 from her $20 wallet balance in order to prove she owns her wallet.

Unfortunately, the Satoshi Test fails - the CASP is expecting funds from Address 3 (the address that Alice's wallet generated when she hit the "Deposit" button in order to add her wallet as a beneficiary in her CASP), but Alice never had any funds on Address 3. Her wallet actually used the UTXO on Address 1 as the input for this transaction. If Alice tries again, the Satoshi Test will again fail: this time her wallet will use her $15 UTXO on Address 2 to construct the transaction that sends $1 to her CASP, and $14 back to herself as change to yet another change address, Address 5. The CASP will again check if funds came from Address 3 and as they did not, the test fails again. Now Alice actually has a $4 UTXO (from her first attempt) and $14 UTXO (from her second attempt) sitting on change addresses (Addresses 4 and 5) that she has never even seen and is not aware that they even exist. And Address 3 still has no usable UTXO. As mentioned, users are not aware of this mechanism going on under the hood.

This whole flow is illustrated by the diagram below:


1. Alice's wallet after receiving funds from Bob and Chen
Alice will not be aware which addresses have UTXOs. She only knows her wallet balance is $20
Wallet: Balance $20
Address 1 : $5
Address 2 : $15
Alice clicks 'Deposit' as she want to add her wallet to her CASP account as a beneficiary. Her wallet generates a new address (Address 3)
2. New wallet state
Address 3 has now been generated
Wallet: Balance $20
Address 1 : $5
Address 2 : $15
Address 3 : $0
Alice adds Address 3 to her CASP account as a beneficiary. Her CASP is required to verify she owns her wallet via a Satoshi Test and asks her to send funds from Address 3 to prove wallet ownership
3: Alice sends $1 to her CASP
Wallet address logic is abstracted away from Alice, she is not aware of it and she cannot control it
Wallet: Balance $20
Address 1 : $5
Address 2 : $15
Address 3 : $0
Address 4: $0
The entire UTXO on Address 1 ($5) is sent (as UTXOs, like coins, cannot be split)
$5
$1
$4
$4 returns as 'change' to a brand new 'change' address generated by the wallet, Address 4
$1 arrives at Alice's CASP
Satoshi test fails: Alice is trying to validate ownership of her wallet, but her CASP sees funds from Address 1, not Address 3, and Address 3 is being used for wallet ownership proof
CASP
4: Final wallet state
Alice is only aware that she has $19, not what addresses hold which balances. If she tries Satoshi test again, it will still fail
Wallet: Balance $19
Address 1 : $0
Address 2 : $15
Address 3 (New) : $0
Change Address 1 : $4

Unfortunately due to a general misunderstanding of how UTXO assets work, it has been assumed that the Satoshi Test can be used as a simple means of verifying wallet ownership, however as discussed, the Satoshi Test will fail in probably >95% of cases for UTXO assets including Bitcoin. And as mentioned, since Bitcoin is still the most popular crypto asset by far with a market dominance of 52% (as of 18th Feb 2024)[3], this is clearly an issue.

And our example is quite a simple case. In the real world, a wallet containing $20 worth of Bitcoin will likely have 100s of tiny UTXOs all sitting on change addresses making up this $20 balance due to the fact that change builds up with wallet usage over time (rather like a penny jar). And so in order to even send just $1, Alice's wallet will need to create a transaction with many of these tiny UTXOs as inputs in order to send the $1 (rather like paying for something costing $1 using one hundred pennies). And the CASP will therefore see 100s of UTXOs as sources of this $1 transaction (from change addresses within the customer's wallet that they will have no knowledge about). And the likelihood is that none of these change addresses correspond to the address being used by the Satoshi test anyway.
This complexity is why wallets handle all this for users in the background. And even in a scenario where Alice somehow stores a previous address she has deposited funds to specifically for use in a Satoshi test, she has no guarantee that the UTXO will still be there by the time the test takes place due to the way that UTXOs are automatically managed by her wallet as described earlier and the way that change functions.

For Account based assets such as Ethereum which have a more traditional approach to transfers and do not use UTXO architecture, the Satoshi Test can work, however due to the fact that a large amount of popular crypto assets including Bitcoin use UTXO architecture, we believe that the methods listed in guideline 69 should be amended to reflect the fact that in many cases a Satoshi Test will not be a viable technical means of verification (and that therefore due to some of the potential problems with the other methods that we discuss below, it will not in fact be possible to find two viable methods for verification using the guideline as currently drafted).

2. Some of the technical means of verification listed (69.e and 69.f) require significant technical expertise by customers, are not often supported by wallets, and introduce the risks of non-technical customers potentially losing funds

The means of verification identified in 69.e and 69.f are:

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;

The most popular wallets such as Coinbase Wallet, Trust Wallet, Atomic Wallet and Zengo etc do not support this functionality. In many cases the reason for this is that these advanced signing features can result in total loss of funds if mistakes are made by non-tech savvy users, and are often exploited by bad actors in order to completely drain customer wallets.

[3] *Ibid.*

This is particularly common with wallets such as Metamask where it is a common occurrence that users mistakenly sign transactions that allow bad actors to completely drain their wallets[4].

In addition, many wallets (e.g. Zengo) are moving towards an MPC based approach[5] (which is actually safer for users due to the fact that poor private key management has been traditionally an area where users were prone to lose funds) where a private key is never created in the traditional sense. *e* and *f* in general would require a large amount of technical expertise on the part of a user, are not widely supported by wallets, and due to the fact that private keys are involved in signing, it is likely that bad actors will exploit lack of user experience in this area and cause significant customer harm.

And in a case where Alice is trying to send her friend Bob funds from her CASP, it is not clear how she could get Bob to verify his wallet using either 69.e or 69.f on behalf of her CASP (or even that Bob is indeed Bob, even if Bob's wallet did support this functionality which most don't).

3. Guidelines 69 and 71 as drafted will hinder the EUs competitiveness as a jurisdiction due to points 1 and 2 without some drafting amendments, and also put EU based CASPs at a disadvantage to CASPs in other jurisdictions such as the UK which has approached self hosted wallet regulation differently

In the UK, the Travel Rule legislation went live on Sept 1st 2023, and now all UK CASPs are required to be compliant. The UK is considered to be a robustly regulated jurisdiction. The UK rules around self hosted wallets are as follows:

Chapter 3 of Part 7A of the Money Laundering, Terrorist Financing and Transfer of Funds (Information on the Payer) Regulations 2017 (SI 2017/692)[6]:

64G.—*(1) A cryptoasset business involved in an unhosted wallet transfer* ***may*** *request from its customer (whether the originator or the beneficiary)—*

(a) such information specified in regulation 64C(5) as it does not already hold; and

(b) where the unhosted wallet transfer is equal to or exceeds the equivalent in cryptoassets of 1,000 euros in value (taken together with any other cryptoasset transfer which appears to be linked), and where its customer is the beneficiary, the information specified in regulation 64C(6) in respect of the originator.

(2) ***In determining under paragraph (1) whether to request information from its customer, the cryptoasset business must have regard to—***

(a) the risk assessments carried out by the cryptoasset business under regulations 18(1) and 18A(1); and

[4] Metamask: Signature Phishing Attacks; Metamask: Unauthorised transactions on my account
[5] Zengo: MPC technology vs private keys
[6] https://www.legislation.gov.uk/uksi/2022/860/regulation/5/made

(b) its assessment of the level of risk of money laundering, terrorist financing and proliferation financing arising from the unhosted wallet transfer.

(3) ***In assessing the level of risk under paragraph (2)(b)****, a cryptoasset business must take account of factors including—*

(a) the purpose and nature of—

(i) the business relationship with its customer (whether beneficiary or originator); and

(ii) the unhosted wallet transfer;

(b) the value of the unhosted wallet transfer and any cryptoasset transfer which appears to be linked;

(c) the frequency of cryptoasset transfers made by or to the customer (whether beneficiary or originator) via the cryptoasset business; and

(d) the duration of the business relationship with its customer.

(4) In the event that the cryptoasset business involved in an unhosted wallet transfer does not receive information requested under paragraph (1) it must not make the cryptoasset available to the beneficiary.

Going back to our previous example with Alice, if instead Alice was the customer of a UK based CASP the transaction attempt would proceed as follows:

Alice is a fully KYCed customer of her UK CASP. Her CASP therefore already has all Alice's originator information as required by the Travel Rule. Alice would then attempt to add Address 3 as a beneficiary and add her name as the owner of the beneficiary in this case. No verification of ownership would be required, but the UK CASP is still required to ensure robust risk mitigants are in place prior to a transaction attempt by Alice including specifically:

(c) its assessment of the level of risk of money laundering, terrorist financing and proliferation financing arising from the unhosted wallet transfer.

This can be achieved with a combination of factors including:

- Blockchain analysis of the complete transaction history of Alice's wallet and any relationship direct or indirect to bad actors (blockchain analysis is particularly effective when used with UTXO assets as risk can be detected at a very granular UTXO level, making it a relatively trivial task to detect risk related to addresses due to the fact that the complete history of UTXOs since the inception of the blockchain can be traced and assessed)
- The duration of Alice's relationship with the CASP in question
- Risk assessment of Alice's behaviour on the CASPs platform via traditional transaction monitoring

- The KYC data the CASP holds for Alice, and any potential red flags if an account review is triggered such as unusual IP addresses, email address concerns, links to other users on the platform and many more
- The collection of the name of the beneficiary Alice is sending to, collected from Alice, which can be then screened using standard name screening tools to assess potential sanctions risk

Assuming the CASP assesses Alice herself to be a low risk user with no particular red flags, and that the self hosted wallet address is low risk from a blockchain analysis perspective, the CASP can allow the transfer to take place with the information it has about Alice and the name of the beneficiary Alice has provided (in this case herself). Additionally, post transaction, the CASP can continue to monitor Alice's wallet for unusual activity via rescreening in case the risk of Alice's wallet significantly increases in future.

From Alice's perspective, she has had a superior user experience with her UK CASP than with her Singaporean CASP and for this reason would be more likely to conduct future transactions with her UK CASP. The UK CASP has a significant advantage over the Singaporean CASP as it is able to remain fully compliant with Travel Rule requirements in a trusted jurisdiction with a robust regulatory framework, mitigate risks associated with self custody wallets effectively, and offer a superior user experience.

Additionally

69.b and 69.c refer to unattended and attended verifications traditionally used in customer onboarding. These are used to prove the customer is who they say they are by comparing photos/videos of the customer with their identification documents in order to confirm identity. It is unclear how these methods could be used to confirm ownership of a wallet however, and as per our previous point, these methods would add a large amount of friction for low risk legitimate users withdrawing to or depositing from wallets that have been assessed as low risk that other jurisdictions such as the UK handle differently, and as mentioned it is unclear how in practice these methods could be used to prove self hosted wallet ownership.

Proposed Amendments

Given the concerns and limitations highlighted above, our amendments are indicated in red below:

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

69.a. advanced analytical tools;

69.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" displaying the address;

69.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";

69.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;

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

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

69.g. requesting the customer attest that the information they have provided about the originator / beneficiary is correct (i.e. self verification) in cases where a combined risk assessment of the customer in question alongside an assessment of the risks associated with the wallet they are transacting with allow the CASP to make a reasonable determination that the self verification their customer has provided can be accepted as a means of verification;

69.h. other suitable technical means as long as they allow for reliable and secure assessment and the CASP is ~~fully~~ reasonably satisfied that it knows who owns or controls the address and that the level of risk of money laundering, terrorist financing and proliferation financing arising from the unhosted wallet transfer is within acceptable limits.

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

Rationale

In the many cases where b, c, d, e and f are not viable, these small amendments provide CASPs the flexibility in certain cases to **allow customers to attest that the details of the originator / beneficiary they have provided are correct i.e self verification**, and allow the CASP to then make a decision based on other factors whether this self verification can be used as a means of verification. Specifically these would be cases where the CASP has assessed the reliability of the customer's self verification to be likely valid based on their overall assessment of the customer's risk profile from a AML/TF perspective using information collected from the customer at the time of onboarding including KYC data, holistic information collected about the customer's usage of the account via transaction monitoring, and an assessment that the originator / beneficiary address is low risk via blockchain analysis.

These small amendments would therefore allow EU CASPs the ability to compete with CASPs from other jurisdictions with robust regulatory frameworks such as the UK on a more even footing, whilst continuing to mitigate the risks associated with self-hosted wallets in an effective and holistic manner.