Before the Arbiter for Financial Services

Case ASF 062/2025

KJ

('the Complainant')

vs

Foris DAX MT Limited

(Reg. No. C 88392)

('Foris', 'the Company' or

'Service Provider')

Sitting of 17 April 2026

The Arbiter,

Having seen the Complaint made against Foris DAX MT Limited relating to its alleged failure to stop the execution of two transfers of digital assets to a fraudulent external wallet involving a self-hosted address[1] despite the introduction of the Travel Rule requirements under Regulation (EU) 2023/1113 (*on information accompanying transfers of funds and certain crypto-assets and amending Directive EU 2015/849*) ('Transfer of Funds (Recast) Regulation' or 'TFR Recast'). The TFR Recast was published in 2023 and, in the case of crypto-asset service providers, is applicable from 30th December 2024.

The Complainant, in essence, claimed that the Service Provider had failed him by being negligent and by failing to properly comply with the TFR Recast, as it:

[1] Article 3(20) of Regulation (EU) 2023/1113 defines a *'self-hosted address'* as follows: *'(20) 'self-hosted address' means a distributed ledger address not linked to either of the following: (a) a crypto-asset service provider; (b) an entity not established in the Union and providing services similar to those of a crypto-asset service provider;'*

i. Failed to verify the accuracy of the information included in his completed form relating to the requested transfer of crypto-assets;

ii. Did not verify the identity of the originator and the true beneficiary (owner of the external wallet) before executing transactions;

iii. Did not apply enhanced due diligence for high-risk/large transactions;

iv. Did not monitor for suspicious transaction patterns;

v. Did not reject suspected transfers;

vi. Still executed a second transfer of crypto-assets to an external wallet after he had first notified them that he had been subjected to a scam.

Complainant claims he made the following asset transfers (excluding fees) in cryptocurrency (USDT),[2] which are the subject of this Complaint:

01.01.2025 USDT 13,945

16.01.2025 USDT 16,035

These were funded by two transfers of fiat currency of €13,800 and €16,300 for the total of €30,100.

Prior to the transfers subject of this Complaint, the Complainant had also made the following transfers to external wallets:

13.12.2024 USDT 195.27

17.12.2024 USDT 497.63

20.12.2024 USDT 5,989.04

However, these payments are not included as part of this Complaint as the Complainant has limited his Complaint with the Office of the Arbiter for Financial Services ('OAFS') to the transactions undertaken after the Service Provider's

[2] USDT known as Tether is *'a stablecoin that is pegged to the U.S. dollar, designed to maintain price stability in the volatile cryptocurrency market by being backed by Tether's dollar reserves'* - https://www.investopedia.com/terms/t/tether-usdt.asp

communication of 27 December 2024, relating to the Company's compliance with the Travel Rule obligations which took effect on 30.12.2024.[3]

By way of compensation, the Complainant is seeking a refund of his loss of €30,000 and a further compensation of €20,000 for extra work, moral damages and stress suffered due to the claimed failures of the Service Provider.[4]

The Complaint as explained by the Complainant[5]

In his Complaint Form to the OAFS, the Complainant submitted that:[6]

> '*The Crypto.com has provisioned a fill in form for transfer of funds to an external wallet without complying to EU anti money laund[ering] regulations, despite claiming in its email of 27th December 2024, that they are going to apply the said regulation from 1st January 2025. The same fill in form mostly suits money laund[ering] or scam money laund[ering] operations, since the Crypto.com did not seek my verification for the accuracy of the said fill in form, for unlawfully passing all its responsibility for compliance with the said regulation to the client, which in many cases are money launder[ers] or scammed money launder[ers], specialised in deceits and lying. Please note the full description submitted by Book of Pleading[7], as well as the EU anti money laundering regulation 2023/1113[8]'*

He further stated that:[9]

> *'By presenting a fill in form, the Crypto.com has transferred its responsibility to the client, despite the fact the EU anti money regulation 2023/1113, clearly says it is the responsibility of Crypto-asset service provider which are summarized as the following: To Verify the identity of the originator and the beneficiary before executing transactions. Apply enhanced due diligence for high risk and large transactions. Monitor business*

[3] Page (P.) 12 & 43
[4] P. 3
[5] P. 1 – 6 and attachments p. 7 - 84
[6] P. 2
[7] P. 17 - 79
[8] P. 80 - 84
[9] P. 3

relationships for suspicious transactions patterns. Reject suspected transfers. Blockchain analytic tools.

Despite me having reported that I believed I had been subjected to a scam money laund[ering] operation on 2nd January 2025, they transferred my fun[ds] of 16045 USDT on 16th January 2025 to the scam money launder[ers] wallet after charging 8% commission for its service.'

Further background

In his formal complaint with the Service Provider of 9 February 2025, the Complainant *inter alia* stated that: [10]

'One of the objectives of the EU regulation 2023/113, is that the financial service company which in this case is Crypto.com should have properly identify, whose is the owner of the wallet to which the fund is intended to be transferred, to identify the risk, to identify the country to which it is being transferred, and so on, to prevent money laundering which it includes scam money. However, in accordance to the enclosed documents, Crypto.com appears to have been negligent towards my interests, by tolerating the scammers.

The enclosed screen shots of my conversation with customer services of Crypto.com in early January 2025, demonstrates, that I have informed the Crypto.com, about the likelihood of a scam, but all I was recommended to denounce it to the local authority, a lengthy process with little rate of success, instead of trying to trace my lost fund, charging the client a reasonable fee for its service.

At the same time, I was also trying to communicate with the customer service of 9bxz.com (the scammers), to reach a peaceful settlement, during which time they assured me by presenting me a guarantee letter supported by Toronto stock market, saying if I could complete their required amount of 30000USDT, I could withdraw all my fund. Another tactic to scam me a second sum of 16045USDT, transferred to their wallet on 16 January 2025. In other words, having known about the scam complaint, the Crypto.com

[10] P. 7

had a second opportunity to block my second transfer on 16 January 2025. Subsequently I discovered the said guaranteed letter was also falsified …'.

In his follow up email of 26 February 2025 to Foris, the Complainant summarised his Complaint as follows:[11]

'On 1st of January 2025, I was drawn in a scam money laund[ering] operation, which it involved buying 13955USDT from the Crypto.com and transfer it to a private wallet which it is used by money launders, believing I was trading with a legitimate company. A similar operation was carried out on 16 January 2025, amounting to 16045usdt. Two scam money laund[ering] operations which they could have been avoided, if Crypto.com, would have properly applied the anti money laund[ering] regulations legislated for all financial services identities in EU …

The same legislation obliges the financial services companies operating in EU, should identify the true owner of the external wallet, whether it belongs to the person himself/herself, or to properly clarify if it is being transferred to a legitimate company, for buying goods or services. It is not sufficient what the client may alleges, but the financial service company should have reasonable evidence whose is the owner of the external wallet, as well as to identify the country it is being transferred …'.

In a subsequent email exchanged with the Service Provider dated 10 March 2025, the Complainant reiterated:[12]

'*Considering that the EU anti money laund[ering] regulations obliges the financial services identities to identify the owner of the external wallets, to which country is being sent, as well as to evaluate the risks. Therefore, would you please reply,* ***what mechanism did the Crypto.com had in place to avoid transferring funds to an external wallet which belong to a terrorist or criminal organization?*** *This is why, when transferring funds through the banks, the first information required to fill in the form is the name of the beneficiary, as well as its address, and the country that is*

[11] P. 10
[12] P. 12 – Emphasis made by the Complainant

> *intended to be send, before the transaction is taking place. An information which is transparent to both parties, as well as the involved bank.*
>
> *Prior to 1st January 2025, I carried out three trading through the same 9bxz.com site with small amounts, however on 27th December I received an email from Crypto.com that the same company is going to comply with the EU regulation of 2024/1113 from 1st January 2025, which gave me more confidence to trade with higher amounts with the said 9bxz.com, believing the Crypto.com is not going to participate with the transfer of funds, if they inspect any irregularities. In other words I trusted the Crypto.com professionalism.*
>
> *I estimate the Crypto.com has made about 2500€ profit for converting my Euros to USDT, which traces the value of US Dollar. In other words it received Euros, and gave back Dollar.* ***I wonder how much this lucrative sum, influence the Crypto.com action, to uphold the client orders, above the EU regulations?'***[13]

In his note to the Complaint Form, the Complainant *inter alia* pointed out that:[14]

> *'In accordance to Crypto.com current mechanism, anyone can register as a client in the same company, to deposit fiat fund in his/her account in the same company and transfer it to an external wallet of anyone or organization anywhere in the world, which it likely belongs to money launders, criminal or terrorist organizations, as long as the same client is paying a lucrative percentage to Crypto.com which is estimated to be around 8%.* ***All he/she needs to do is to tick (select) that he/she is the owner of the same external wallet, without ever being asked for a verification by Crypto.com team****'*.

In the same note, the Complainant referred to *'regulation 2023/1113'* and affirmed that *'Crypto.com had no effective measures to properly comply with the same regulations'* submitting that *'As [a] result it has caused the plaintiff an apparent loss of some 30000€'.*[15]

[13] Emphasis made by the Complainant
[14] P. 19 - 24
[15] *Ibid.*

The Complainant further submitted that this loss *'could have been prevented if the Crypto.com had properly applied the EU anti money laund[ering] regulations'*.[16]

In the same note, the Complainant *inter alia* noted that on 1 January 2025, he transferred USDT to a wallet belonging to the company *9bxz.com*. In the Crypto.com form, he had ticked that he was the owner of the listed wallet to which the USDT were to be transferred. He explained that:

> *'However in reality the same wallet belonged to 9bxzx'*, highlighting *that 'The law requires that it is the duty of the financial service company to identify the true owner of an external wallet, but in practice the Crypto.com … has passed this crucial duty to the client, which is the main reason for its negligence'*.[17]

The Complainant further explained in the said note that after transferring USDT to a wallet of *9bxz.com* on 1 January 2025, he surprisingly discovered that he could not trade and was then requested by the customer representative of *9bxz.com* to deposit more funds to be able to withdraw his money. He claimed that: [18]

> *'…To me it appeared as a scam, since such invisible rule had not been noticed in their website [of 9bxz.com] in advance…*
>
> *I immediately informed Crypto.com, explaining my experience requesting their help to trace my fund. All they could say, that I should go to my local authority, as well as promising that they are going to take the preventive measures for any future attempt, so a similar ordeal will not occur again ...* ***However we can observe that on 16 January they repeated the same negligence, and their procedures for identifying the true owner of an external wallet as well as to evaluate the risks, were no[n] existent and remained the same as before***.'
>
> *The Crypto.com second negligence can be observed by viewing document 7.2 again. In that form there is only one option available leading the client*

[16] *Ibid.*
[17] P. 21
[18] P. 21 & 51

to tick, that he/she is the owner of the destined wallet, without asking any evidence from the client. In other words the client is leaded to tick the said box for moving forward, and since the Crypto.com does not ask for any evidence, the fund can be transferred to a non custodian wallet which it may belong to anyone. ***So again the crucial and sensitive responsibility of the Crypto.com to identify the risks, has been passed to the client, without any real evaluation, despite the law which clearly state it is the responsibility of the financial service company****'*.[19]

Service Provider's reply

Having considered in its entirety the Service Provider's reply,[20] where the Service Provider provided a summary of the events which preceded the Complainant's formal complaint and submitted the following:

1. *Background*

- That Foris Dax MT Limited offers the following services: a crypto custodian wallet ('the Wallet') and the purchase and sale of digital assets through the Wallet. Services are offered through the Crypto.com App ('the App'). The Wallet is only accessible through the App and the latter is only accessible via a mobile device.

- That the Service Provider additionally offers a single-purpose wallet ('the Cash Wallet') (formerly referred to as the Crypto.com Fiat (EUR) Wallet), which allows customers to top up and withdraw fiat currencies from and to their personal bank account(s). This service is offered by the legal entity Foris MT Limited.

- That the Complainant became a customer of Foris DAX MT Limited through the Crypto.com App and was approved to use the Wallet on 2 December 2024.

- In the submitted complaints file, it notes that the Complainant outlined his desired remedy as reimbursement for incurred financial losses.

[19] Emphasis made by the Complainant
[20] P. 91 – 98 with attachments p. 99 - 104

2. *Timeline*

The Service Provider provided a timeline for the transactions of the Complainant's account.

The following deposits into EURO and purchase of USDT were indicated:

- Deposit of 200 EUR to his Cash Wallet on 11 Dec 2024 and purchase of 205.27 USDT on 12 December 2024;
- Deposit of 500 EUR on 17 Dec 2024 and purchase of 507.63 USDT on the same date;
- Deposit of 6,000 EUR on 20 Dec 2004 and purchase of 6000 USDT on the same date;
- Deposit of 13,800 EUR on 31 Dec 2004 and purchase of 13,970.42 USDT on 1 Jan 2025;
- Deposit of 16,300 EUR on 16 Jan 2025 and purchase of 16,045 USDT on 16 Jan 2025.

The Service Provider then listed all the transfers (for the total amount of 36,661.94 USDT) that were made between 13 December 2024 and 16 January 2025 from the Complainant's Crypto.com Wallet to an external wallet address.

Three transfers were made in December 2024 to an external wallet (excluding withdrawal transaction fee of between 10-11 USDT per transaction) as follows:

13.12.2024 USDT 195.27

17.12.2024 USDT 497.63

20.12.2024 USDT 5,989.04

Two transfers were then effected after 30.12.2024 (excluding withdrawal transaction fee of 10 USDT per transaction) as follows:

01.01.2025 USDT 13,945

16.01.2025 USDT 16,035

The Service Provided noted that the external wallet addresses were as follows:

- Ox226ff029ddbaef56cfd7789e6d25a0beeb40855c
- Ox7ce977846aa7d114290b348d44568d2c236403e4
- Ox7e803c00db4e3f623e8ba56616a83c418699ccad
- Ox98923090263cf97452cbe5581dd2d5fldc72e3cd
- Ox6772eecl7bcd48bfd6ef660a87952f74032a2009

The Company submitted that based on its investigation, it has concluded that it is unable to honour the Complainant's refund request based on the fact that the reported transfers were made by the Complainant himself.

The Service Provider noted that whilst it sympathises with the Complainant and recognises that he may have been misled or induced into transferring funds to an alleged fraudster, it is important to note that these transfers were made solely at the Complainant's request.

It also emphasised that the addresses the funds were transferred to, do not belong to the Company and as such, any due diligence of the ownership of these addresses falls under the responsibilities of the provider of the said wallets.

It further noted that, unfortunately, Crypto.com cannot revoke any virtual asset withdrawals because blockchain transactions are fast and immutable.

The Service Provider further submitted that the Complainant is solely responsible for the security and authenticity of all instructions submitted through his Wallet as outlined in the Foris DAX MT Limited Terms of Use. It referred to the relevant section of the Terms of Use which it quoted as follows:

> *'QUOTE*
>
> *6.2.*
>
> *Without prejudice to the foregoing and any other terms in these Terms, we assume that any and all instructions received from your Enabled Device have been made by the rightful owner. You are solely responsible and liable for keeping your Enabled Device safe and maintaining adequate security and control of your login and authentication details (including, but not*

limited to, your username, and password), and shall likewise be solely responsible for any access to and use of the Crypto.com App and the Services through your Enabled Device, notwithstanding that such access and/or use may have been effected without your knowledge, authority or consent. We will not be liable to you for any loss or damage resulting from such access and/or use.

…

7.2. Digital Asset Transfers

…

(b) Crypto.com processes all Digital Asset Transfers according to the Instructions received from you and does not guarantee the identity of any recipient. You should verify all transaction information prior to submitting Instructions for a Digital Asset Transfer to Crypto.com as the Digital Asset Transfer may not be cancelled or reversed once processed by Crypto.com unless Crypto.com decides at its sole discretion that the transaction should be cancelled or reversed and is technically capable of such cancellation or reversal. You acknowledge that you are responsible for ensuring the accuracy of any Instructions submitted to Crypto.com and that any errors may result in the irreversible loss of your Digital Asset.

…

UNQUOTE'.

The Service Provider, in summary, concluded that it seems conceivable that the Complainant has been the victim of an alleged scam. However, due to the nature of the external wallet and the fact that it is not hosted or operated by the Company, the Service Provider can neither confirm nor deny this.

It explained that whilst it fully empathises with the Complainant in this regard, it cannot be overlooked that he had willingly transferred his virtual asset holdings from his Crypto.com Wallet to external wallet addresses which he nominated.

The Service Provider reiterated that as outlined above in the Foris DAX MT limited Terms of Use, the Complainant is solely responsible for the security and

authenticity of all instructions submitted through the Crypto.com App, and as such, the Company cannot accept liability for the veracity of any third-party or for the instructions received from the Complainant themselves.

Hearings

During the first hearing on 17 June 2025, the Complainant testified as follows: [21]

> *'Solemn Declaration of [the Complainant]:*
>
> *Having studied the response letters sent by the Foris DAX Malta, I have summarized the points of disagreements with the same financial service provider, which are noted in the following. I reiterate, I have no complaints about my transactions with the said company before 1 January 2025. Although I have supplied the OAFS a comprehensive history description of my trading with Foris DAX Malta, my main complaints are concerned with two transactions taken place on 1 January 2025 and 16 January 2025, carried out under application of EU Regulation of 1113/2023. I also reiterate I had no direct dealings with a company named 9bxz.com.*
>
> *1. The preference of EU anti-money laund[ering] regulation of 1113/2023 (Travel Rule), over the client's order for transfer.*
>
> *I believe in proper consideration that the application of law should have the priority over the client´s orders or wishes. In other words, the law should not be overridden by the client´s wishes or the service provider rules and conditions. However, in accordance with the Crypto.com practice, the same anti- money laund[ering] regulation could be disregarded in order to satisfy the client´s order, which it involved earning some 8% commission as well. A Regulation which Crypto.com, in its email of 27 December 2024, has stated it is going to comply with from 1 January 2025. In my book of pleading, I have substantiated how with a bit of care and diligence, the Crypto.com was enabled to comply with important requirements of the said law, if they had wished so. I believe not complying with the verification requirement is the said service provider's first negligence.*

[21] P. 105 - 108

To expand about the verification process, I recall my registration process when I became a client of Foris DAX Malta. After filling in the form, in which I had written my name and surname, as a matter of verification, the same company asked me to forward a copy of my passport, and then take a picture of myself via app to verify whether it matched with the picture in my passport or not. So, I believe the same service provider understands what the verification process means.

2. The transfer of its duty and legal obligation to the client

According to my experience, Foris DAX Malta Limited, by its own self design fill-in form has attempted to pass the same vital duty and obligation of verification of the true ownership of the external wallet to the client which effectively means an attempt to neutralise all anti-money laund[ering] regulations.

In accordance with the same practice, anyone can send funds to anyone or any organisation anywhere in the world, as long as the client ticks that he/she is the owner of the external wallet and pays a high commission of some 8% to Crypto.com, because the said firm never complied with the verification process to identify who is the true owner of the external wallet to whom they are sending the funds.

In order to quantify their negligence, I believe the following example may be helpful. Assuming a security firm is employed to verify who is entering and exiting the premises, the security firm, however, passes this vital obligation and duty to the clients themselves to identify their entries and exits for exchange of a commission. Do we consider the action of the security firm as negligence, or we classify it as outrageously illegal?

3. To evaluate the risks by identifying the jurisdiction to which the funds are being transferred

Other requirements of the same anti-money laund[ering] regulation, oblige the service provider to identify to which jurisdiction or country the funds are being transferred so the client is better informed of the risks involved; a legal requirement that Foris DAX Malta Limited did not comply with.

The said company may allege that a pop out message did appear asking me whether I trusted the wallet the funds were going to be transferred to. A message which I do not recall having ever seen it. Hypothetically speaking, even if such message did appear during my transfers, it is not even close to the compliance required by the law which clearly demands the jurisdiction to be identified prior to the transfer so that the client can better evaluate the risks involved. I believe this is the second case of negligence committed by Foris DAX Malta Limited.

4. <u>Monitoring the business relationship for suspicious transaction patterns</u>

Another requirement of the same law obliges the financial service provider to monitor the business relationship of the client for suspicious transaction patterns. A task that Crypto.com did not comply with either.

On 2 January 2025, I reported to the customer service of Foris DAX Malta that I had been subjected to a scam on 1 January 2025, which could have been avoided if the said company had complied with the EU regulation. The customer service of the same company replied, which I quote in the following, which is enclosed as document 8 in page 35 of my book of pleadings:

> *"Thank you again for reporting the case and providing us with all the necessary information to take preventive measures against future attempts."*

However, Foris DAX Malta Limited transferred my funds amounting to 16045 USDT on 16 January 2025, with exactly the same procedures as always in the past which is an additional discrepancy between the statements and the actions taken. I believe this is the third case of negligence committed by Foris DAX Malta Limited. In fact, having revised the fill in forms and procedures taken by the same financial service provider, we discover that the same procedures remained the same as prior to 1 January 2025. Having considered that the same company carried out two transactions on 1 January 2025 and 16 January 2025, and for each transaction committed at least three cases of negligence, therefore, we can consider that it committed some five to seven instances of negligence during the same two transactions.

Conclusion:

Your Honour, due to the said cases of negligence, I lost €30,000, which could have been avoided if Foris DAX Malta Limited had truly complied with EU anti-money regulation 1113/2023 which, according to their statements, was going to be applied from 1 January 2025. Therefore, I request the Honourable Arbiter to direct Foris DAX Malta Limited to compensate for my loss of €30,000 as well as the additional payment of €20,000 for legal costs and for the stress that their negligence has caused us so far.'

At the hearing of 16 September 2025, there was a long cross-examination of the evidence that the Complainant had given in the previous hearing.[22] The main points emerging were that the:

1. Complainant confirms that he wanted to carry out the transactions and so authorised the payments by ticking accordingly. He filled a form sent by Foris declaring himself as the beneficial owner to the external wallet. He said at the time he did not really know what made the wallet external and what this meant.

2. Complainant argued that notwithstanding that he declared, under the guidance of the scammer, that he was the owner of the external wallet, Foris still had a duty to make verification in terms of the Travel Rule that he was really the beneficial owner. He said it defeats the scope of the Travel Rule if the Service Provider simply accepts a tick box which the victim makes under the direction of the scammer.

3. Complainant admitted that *Crypto.com* (brand name of Service Provider) had warned him about possible fraud about an initial transfer of $200 but he disregarded the warning as it was generic and as he had recovered the small amount involved where he received two paybacks from the scammer and earned about $500 in 2024.[23] Furthermore, the wallet address of the last two transfers subject of this complaint was different from the one about on which he received a suspicion report.

[22] P. 113 - 120
[23] P. 117 - 118

4. The Circular of 27 December 2024 from the Service Provider about greater transparency following the introduction of the Travel Rule gave him confidence to invest larger amounts.

5. Complainant had filed a report with the Spanish Authorities.[24]

A third hearing was held on 04 December 2025, for the proofs of the Service Provider, where an official representing the Service Provider stated:[25]

'The complainant … became a client and user of the service provider on the 2nd of December 2024.

The disputed transactions in question relate to withdrawal of cryptocurrency, which was purchased on the Crypto.com App, to two different external wallet addresses on the 1st and 19th of January 2025.

These wallet addresses are what we call non-custodial addresses, which means that they are not serviced by Crypto.com or identified from the blockchain as provided by service providers of a similar nature. The evidence at hand and the agreement of the complainant shows that these transactions were fully authorised by himself.

At the time of the withdrawals, none of the address wallets in question were subject to any warnings from our own internal investigations or any third-party transaction monitoring tools that we use. I would like to highlight the applicability of the Travel Rule in this situation, given they occurred post-implementation of such. The complainant was requested to complete a Travel Rule form or declaration which asked the user to identify whether the external wallet to which funds were transferred was self-hosted or otherwise, and to specify the beneficiary of the external wallet as the crypto asset service provider of the originator.

The service provider obtained and maintained the information required under the Travel Rule regulation. This included the name of the beneficiary, the beneficiary's distributor ledger address or wallet address, and the unique transaction identifier of the wallet address. Each transfer initiated by the user

[24] Complainant provided copy of original Police Report in Spanish and, also, an English translation (P. 122 – 132)
[25] P. 137 - 139

could therefore be identified individually. This can be seen from the evidence that [the Company's lawyer] submitted earlier this morning.

The Arbiter would like [the Service Provider] to explain exactly this evidence.

[The official from the Service Provider] continues:

So, this would have been the form that the complainant would have seen when filling in the whitelisting details. When he whitelisted an address post-Travel Rule, and with the two transactions in question, he would have had to fill in this form.

As per this form, the complainant indicated that he was the owner of this wallet address and that this was a non-custodial wallet. This can be seen from the other two screenshots that are labelled 'Entitled Transaction'.

So, these are screenshots of the two related transactions involved. As you can see, there is the time stamp of one of the transactions which was made on Wednesday, 1 January 2025.

And you can also see the amount underneath and the wallet address, to address. It is shortened here. But at the bottom where you can see five rows of data, you can see in the first row address and it shows the wallet address to which the funds were sent. Then, in the third row, you can see towards the middle, Travel Rule Recipient First Name: [first name of Complainant], Travel Rule Recipient Last Name: [last name of Complainant], meaning that it belonged to [the Complainant].

If we go to the next transaction, you can see that it occurred on 16 January for 16,045 USDT.

The address can also be seen in the first line of the five rows of information at the bottom. Also [the Complainant] again indicated that he is the recipient of the address, being Travel Rule Recipient First Name: [first name of Complainant], Travel Rule Recipient Last Name: [last name of Complainant], Travel Rule Recipient Name: [the Complainant], and that he was the true owner of the said wallet.

The Arbiter states that, if he understands correctly, these transfers to these wallets, which later turned out to be fraudulent wallets, [the Complainant] ticked the box where he confirmed that he was the owner of these wallets.

And that, according to the Service Provider, this is sufficient defence that by accepting that declaration, you satisfy the Travel Rule obligations which we know about, that you have to take certain action to ensure that these were transferred to a known beneficiary of the receiving wallet.

Asked by the Arbiter whether this is correct, [the official representing the Service Provider] confirms that this is correct.'

Answering questions from her Lawyer, the representative of the Service Provider continued:[26]

'I am being asked if the user having ticked the box which is not a self-hosted wallet and indicated that this is a third-party wallet whether he would have been directed to another screen or whatever, which would have required further information if he did not tick self-hosted.

I say, yes, that is correct. He would have been directed to a separate screen which would have required him to enter the recipient's first name, last name, country, and the wallet type. Yes.

It is said that with regards to the correspondence sent on 1 September 2025, the Complainant alleged that he received this email a year later after the implementation of the Travel Rule came into force, whereby he is saying that this was the communication he received with regards to the adherence of the Travel Rule.

Asked to explain what this email of 1 September 2025 was, and whether actually Crypto.com took into consideration Travel Law a year later or was there any information sent before to users to make sure that they are compliant with the Travel Rules, I say that the service provider would like to state on record that this email, as you can see from the email address itself and the text of the body, is an email sent by the Crypto.com Exchange. Now the Crypto.com Exchange is a completely different service and product that is

[26] P. 139 - 141

provided by a Cayman Islands registered entity and is completely irrelevant to the Crypto.com App and any of the transactions that this complaint involves.

It is being said that on page 43 of the complaint, the complainant submitted an email which is dated 27 December 2024, whereby Crypto.com informed users that it would be introducing several measures to comply with the Travel Rule.

Asked whether this form filling and this extra additional step one of these additional measures that Crypto.com had done prior to the implementation of the Travel Rule, I say, yes, this was implemented once the Travel Rule was in practice.

Asked whether the complainant was given any warnings apart from all this verification process and assessment through the Travel Rule; whether, regardless of all this, was the user given any warnings before the transactions and withdrawals made, I say, yes. Now, it has not been submitted yet before the Arbiter but this can be submitted after the hearing: with regards to warnings, in the course of the complainant's disputed transactions, the service provider had provided numerous warnings regarding withdrawals to external wallets.

The first of these warnings had appeared when the user was adding a new withdrawal address to the Crypto.com App at the whitelisting stage. Now, this takes the stage of a full pop-up screen as well. This and a similar warning would appear at the time of each subsequent withdrawal, whether or not the withdrawal address had been newly whitelisted, or a withdrawal had already been made previously.

Both pop-up warnings specifically warned the complainant against scams and to not whitelist or withdraw digital assets to, for example, investment platforms touting unrealistically high returns, people the complainant did not know well, and to any source the complainant did not have complete confidence in.

In respect of the warnings displayed during the withdrawals, the complainant is further warned that the withdrawal was irreversible. The complainant was also encouraged to learn more about safety and protection from scams by

clicking the link 'Learn More'. This link takes users to the regularly updated Crypto.com Help Centre page avoiding digital currency scams.

Upon the complainant confirming that he had read the scam warnings by clicking on the 'Confirm and Withdraw' button on the pop-up warning, the complainant confirmed he had accepted the risks involved and took full responsibility for the withdrawals to the external wallets. He specifically agreed to and acknowledged that the withdrawals were irreversible and that the service provider would not be liable for assets sent to the external wallets. And in spite of these numerous warnings mentioned above, the complainant proceeded to make withdrawals to the external wallets.

It can be said that the complainant either negligently disregarded the warnings or completely ignored them. As mentioned at the beginning, these screenshots can be provided to the Arbiter if he so wishes.

Lastly, I would like to add that there was nothing once again in our own controls, as well as the controls of our third-party employed tools, to indicate that there was any malicious or scam activity involved in these cases, in the withdrawals at the time that they happened. Nothing was communicated to or brought to the attention of the service provider by the complainant concerning these transactions until they had already been completed.

In so far that the transactions have been completed to the full satisfaction of what we were asked to execute on behalf of the complainant, the service provider submits that we do not have responsibility with regards to these transactions.'

The Complainant then affirmed that the generic warning which were given before the coming into force of the Travel Rule are irrelevant as what matters is what additional measures did Foris take to honour their obligations under the Travel Rule.

He maintained that a tick box declaring ownership by a complainant/victim of a scam was not really what the Travel Rule expected from the Service Provider.

Final submissions

The Complainant informed that he is resting on his evidence and will not be making final submissions.

In their final submissions, the Service Provider reiterated:

1. That the Complainant's loss was the result of his gross negligence in not taking precautions to verify the credentials of those who were leading him to make investments.

2. That he was given all the usual warnings (which he ignored) at the stage of whitelisting the external wallet addresses and each time he made a transfer to such wallets.

3. The additional obligations introduced by the Travel Rule.

   Given that the new Travel Rule obligations represent the core subject of this Complaint, the Arbiter is reproducing the related paragraphs in the final submissions of the Service Provider with respect to this point:

   'Risk Assessment and Transaction Monitoring under the EU Regulations

   22. *For the avoidance of any doubt, the Respondent submits that the internal monitoring procedures of the Respondent are fully in line with the requirements as required under the FIAU Implementing Procedures.*

   23. *The Respondent would first highlight that the Respondent is fully compliant under the AML, CFT and KYC laws and regulations that the Respondent is subject to, including the Prevention of Money Laundering and Funding of Terrorism. This includes comprehensive internal monitoring, account monitoring and external reporting procedures. As already emphasized above, no evidence has been provided to show that the External Wallets had been flagged at the material time the Disputed Transactions occurred.*

   24. *At the material time, the Respondent had no knowledge that there was any fraud history linked to the External Wallet. As has been submitted by the Respondent and unchallenged by any*

contemporaneous evidence offered by the Complainant, the wallet in receipt of the funds subject to the Disputed Transactions was not labelled by any transaction monitoring system (whether the Respondent's own or through third party vendors) as a wallet suspected of illicit behaviour at the time of the Disputed Transactions.

25. *In respect of transaction monitoring as it relates to the Disputed Transactions, it is submitted that the Respondent has carried out due monitoring of these transactions as they were performed. However, due to its overarching obligations due to the FIAU in respect of transaction reporting, the Respondent is not at liberty to share details of the internal monitoring results for any individual cases.*

26. *Nonetheless, it is respectfully submitted that the Arbiter is not the competent authority to adjudicate or hear allegations relating to AML and CTF matters as these should be dealt with by the FIAU in accordance with Chapter 272 of the Laws of Malta.*

27. *With regards to the application of the travel rule through Regulation (EU 2023/1113) on information accompanying transfers of funds and certain crypto-assets (the* ***"Travel Rule Regulation"):***

    By way of background, the Respondent submits that Regulation (EU) 2023/1113 became applicable on 30 December 2024. The Regulation recasts Regulation (EU) 2015/847 and brings the EU's legal framework in line with the Financial Action Task Force (FATF's) standards by extending the obligation to include information about the originator and beneficiary to Crypto-Asset Service Provider's (CASPS) - the Travel Rule Regulation. As per Article 1 of the Travel Rule Regulation, the subject matter of the Travel Rule Regulation is to, inter alia, "lay down rules on the information on payers and payees accompanying transfers of funds, in any currency, and on the information on originators and beneficiaries accompanying transfers of crypto-assets, for the

purposes of preventing, detecting and investigating money laundering and terrorist financing, where at least one of the payment service providers or crypto-asset service providers involved in the transfer of funds or transfer of crypto-assets is established or has its registered office, as applicable, in the Union". The Travel Rule Regulation is not aimed at preventing, detecting and/or investigate fraudulent activities. The Travel Rule Regulation forms part of wider anti-money laundering obligations to have effective procedures in place to detect and prevent money-laundering, terrorist financing and proliferation financing. On this basis, the Respondent submits that the Compliant does not have a legal basis in terms of the Travel Rule Regulation.

28. *One must also bear in mind that the information obtained by the Respondent is subject to strict data protection rules in terms of the General Data Protection Regulation (Regulation (EU) 2016/679). Generally, in order to be able to process data for a specific purpose, the Respondent is to have a legal basis for the processing such data. The Travel Rule Regulation does not provide a legal basis for the processing of such data for fraud related purposes and therefore, the legal basis being used by the Complainant does not hold.*

29. *Notwithstanding and without prejudice to the above, the Respondent submits that in the context of this Complaint, the Complainant is making reference to Travel Rule Regulation. The Respondent, without prejudice to the above, [submits] the following:*

    The identification of external wallet data is established through provisos of Article 14(5) and 16(2) of the Travel Rule Regulation (Identification of a transfer from or to a self-hosted wallet):

    a) *Article 14(5) of the Travel Rule Regulation provides as follows:*

        "In the case of a transfer of crypto-assets ***made to a self hosted address,*** *the crypto asset provider of the originator shall obtain and hold the information referred to in paragraphs 1 and 2 and*

shall ensure that the transfer of the crypto-assets can be individually identified.

Without prejudice to specific risk mitigating measures taken in accordance with Article 19b of Directive {EU} 2015/849, in the case of a transfer of an amount exceeding EUR 1 000 to a self-hosted address, the crypto-asset service provider of the originator shall take adequate measures to assess whether that address is owned or controlled by the ***originator."***

Similarly, Article 16(2) of the Travel Rule Regulation provides that:

"In the case of a transfer of crypto-assets ***made from a self-hosted address,*** *the crypto-asset service provider of the beneficiary shall obtain and hold the information referred to in Article 14/1) and (2) and shall ensure that the transfer of crypto-assets can be individually identified.*

Without prejudice to specific risk mitigating measures taken in accordance with Article 19b of Directive {EU} 2015/849, in the case of a transfer of an amount exceeding EUR 1 000 from a self-hosted address, the crypto-asset service provider of the beneficiary shall take adequate measures to assess whether that address is owned or controlled by the beneficiary."

With regards the above legal provisions, the Respondent obtained written confirmation from the Complainant that the transfer and transaction pertaining to the Disputed Transaction was a transfer made to a wallet which the Complainant declared to be 'self-hosted' in compliance with paragraph 78 of the Travel Rule Regulations which adds that "if such information cannot be retrieved via technical means, the originator's CASP and the beneficiary's CASP should obtain that information [i.e. the terms of whether the counterparty wallet to the CASP is self-hosted or not] ***directly from its customer."***

The Respondent submits that it should not be held liable and responsible for any misstatements made by the Complainant. The Complainant was required to provide true and accurate information, however, has provided inaccurate information and is now claiming that Respondent should be the consequences of transfers which were instructed and authorised by the Complainant.

It is to be understood that the purpose behind the Travel Rule requirements in terms of the Travel Rule Regulation is for the Respondent to identify the nature/type of wallet from/to where the crypto-assets are being sent. Apart from satisfying the legal requirements in terms of the applicable provisions outlined above, the Respondent also implements checks to ensure fraud-related control, wherein wallets identified by the users are tracked for fraudulent activity through blockchain monitoring tools.

b) *In addition to the above, the Respondent makes reference to the proviso of Article 16(2) of the Travel Rule Regulation which provides as follows: "Without prejudice to specific risk mitigating measures taken in accordance with Article 19(b) of Directive {EU) 2015/849, in the case of a transfer of an amount exceeding EUR 1000* ***from*** *a self-hosted wallet address, the crypto-asset service provider of the beneficiary shall take adequate measures to assess whether* ***that address*** *is owned and controlled by the beneficiary." Therefore, in relation to transfers of crypto-assets* ***from*** *a self-hosted wallet, the Travel Rule Regulation that the CASP* ***of the beneficiary*** *shall take adequate measures to assess whether the address from where the crypto-assets are being sent is owned and controlled by the customer.*

30. *In this case, the Respondent makes reference to page 115 of the Complaint file wherein the Complainant stated the following:*

"Asked whether it is correct to say that this form was sent to me by Crypto.com, I say yes. Asked whether it is correct to say that I was asked to fill in this form by Crypto.com, I say, yes.

Asked whether it is correct to say that I was asked to send this filled in form and send it back to Crypto.com, I say, yes.

Asked whether it is correct to say that I filled in this form myself, I said that I filled the form myself in accordance to the guidance I used to receive. At the time, I hardly had any knowledge about external wallets. I didn't understand all these things. The thing is, I was being sent by my other phone, what should I learn, and what should I do to proceed.

Asked whether I asked any questions about how to fill in this form from Crypto.com or whether I asked my tutor, I say, no.

Asked whether it is correct to say that in this particular form, where I was asked information, I indicated myself as the owner of the external wallet, I say, yes, I did."

And page 116 of the Complaint file:

"It is being said that I declared that it was me who hosted that wallet, I say, yes.

It is being said that I declared myself as the owner of the wallet that I was sending."

Through the form which was completed by the Complainant the following information was retrieved:

(i) The name, customer identification number and address of the originator

(ii) The name and identification number of the beneficiary (which is the same as the originator since the Complainant declared that the wallet was self-hosted) and

(iii) The wallet address and unique identifier of the beneficiary

This information was deemed complete and accurate in terms of the Travel Rule Regulation and thus processed and retained. This was confirmed by the Respondent on page 138 of the complaint file wherein it was stated that:

> *"The complainant was requested to complete a Travel Rule form or declaration which asked the user to identify whether the external wallet to which funds were transferred was self-hosted or otherwise, and to specify the beneficiary of the external wallet as the crypto-asset service provider of the originator.*
>
> *The service provider obtained and maintained the information required under the Travel Rule regulation. This included the name of the beneficiary, the beneficiary's distributor ledger address or wallet address. Each transfer initiated by the user could therefore be identified individually."*

The Respondent submits that the Complainant himself personally completed and signed the relevant Travel Rule form sent by the Respondent, in which he expressly stated that he is the owner of the external wallets in question. By providing this information directly, the Complainant made a clear and affirmative representation as to the ownership and control of the wallet addresses.

31. *In reliance on the Complainant's own declaration, the Respondent satisfied the applicable Travel Rule Regulations, which permit reliance on reliable and secure information provided by the Complainant for the purpose of assessing ownership and control of the external wallets in question. On the basis of the information supplied by the Complainant, the Respondent was satisfied that it knew who owned and controlled the relevant wallet address.*

32. *The Complainant must therefore bear responsibility for the accuracy and completeness of the information he voluntarily provided. The Respondent was entitled to rely on the Complainant's explicit confirmation of ownership and was under no obligation to raise additional questions where the customer unequivocally identified himself as the wallet* ***owner.***

33. *Accordingly, the Respondent acted reasonably, lawfully and in full compliance with its regulatory obligations by using the information exactly as it was provided by the Complainant, without seeking further clarification were none was warranted.'*

Having heard the parties

Having seen all the documents

Considers

Complainant's profile

The Complainant was born in Iran in 1957. He was 67 years old and resided in Spain at the time of the disputed transactions.[27]

Background about the Scam

In an attachment to his Complaint Form to the OAFS, the Complainant described the scam as follows:[28]

> *'In December 2024, I knew very little about digital currency transactions, but through a scam chat tutor I was introduced to Crypto.com as well as 9bxz.com companies, for a legal commercial activity which it involved buying USDT from the said company and sell it in the website of another company named as 9bxz.com known as secondary market, for a higher price at right time, making a legal profit once the corresponding taxes are paid.*
>
> *…*

[27] P. 122
[28] P. 19 - 23

I initiated with small amounts for which I received payments next day in December 2024 …

… all my operations were guided by my ex-scam tutor …

…

On 1st January 2025 … USDT was deposited in the 9bxz.com wallet … but surprisingly I could not trade it. The customer service of the same company stated that because of my raise[d] client's category to VIP2, I have to deposit minimum 40000 USDT, before being able to withdraw it …

…

… I was trying to reason with customer service of 9bxz.com a withdraw negotiation for my 13955USDT. But they were determined as well as promising that once I complete the minimum amount of 40000USDT, I will be able to trade and withdraw my fund. They even produced a guarantee letter supported by Toronto Stock Exchange, that if I complete the 40000USDTt, I will be able to withdraw my fund … Subsequently, I discovered the same guarantee letter is also falsified.

At this stage my tutor, whom at that time I still had not suspected to be a member of scam money launder[ing] organization, encouraged me to apply for a second borrowing, assuring me the problem would be easily resolved if I could complete the 40000USDT. Since I could not get a second loan for 26000€, she offered to invest 10000USDTt to be added to my USDT account in 9bxz.com, and then withdraw our fund paying her share of profit.

At the time I could not [find] any quick solution to the matter, and considering the guarantee letter of 9bxz.com supported by Toronto Stock Exchange, as well as my tutor, I applied for a loan, and transferred 16300€ to my euro account in Crypto.com …

On 16 January 2025, I repeated the same process as the 1st January 2025, and bought 16045usdt from Crypto.com and transferred it to the wallet of 9bxz.com. My tutor also transferred 10000usdt to my usdt account in the said company … This time I was able to trade it and the sale amount of 43480€ was deposited in my Euro account in 9bxz.com …

…

Since 16 January 2025, I tried to reason again with customer service of 9bxz.com to withdraw my fund, even offering them to leave the profit made for themselves, and only let me to withdraw my 30000USDT, but they were persistent that the only way to withdraw my fund would be to bring in another 40000USDT for trading which I knew for sure, it is another scam.

On 27th January 2025, after exhausting all possible means, to reach a compromise with 9bxz.com, I made a formal complaint against the said company to the Guardia Civil Almuñécar, accompanied with some 30 pages of evidence, as well as to hand over my phone in which the [whatsapp] chats with the same scam tutor had been registered …'.

Further background on how the scam was perpetrated emerged from the criminal proceedings initiated by the Complainant with the Spanish authorities.[29] The interaction with the scammer was, in such proceedings, described as having initially started from a message received by the Complainant from a person who identified herself as *'Ellie'* on Whatsapp, where she first enquired about a property for sale. After continued conversations, she eventually told him she was *'earning money by buying and selling digital currency'* and after him expressing interest, she started *'teaching him how to make the investments'*, first starting with *'small investments'* and *'obtaining returns quickly'*.[30] It was further described:

'That [the Complainant] has had to install the software called TMXB on the telephone, which connects to the Internet from the URL 9bxz.eom/#/, this being the means of access to the operations described above. That through the WhatsApp application, this woman called Ellie sent the complainant screenshots of how to carry out the process on the page described above'.[31]

The Arbiter has no reason to doubt the veracity of the Complainant's claims and is satisfied, even on the balance of probabilities, that the Complainant was a victim of a scam. No reasonable doubts have been raised or emerged to the contrary. Consideration has been given to various factors, including: the nature

[29] P. 122 - 123
[30] P. 123
[31] *Ibid*.

and credibility of the events outlined in the Complaint and the ensuing proceedings; the solemn declaration of the Complainant, testimony and evidence produced; the communications with the scammer;[32] the report/ initiation of criminal proceedings made by the Complainant dated 27 January 2025.[33]

The Arbiter shall next proceed to consider the new obligations applicable to the Service Provider with the introduction of the Travel Rule.

New additional responsibilities

This is the first complaint being adjudicated by the Arbiter which tests the additional responsibilities of a service provider licensed under the VFA Act/ MICA regulatory regime (Regulation on markets in crypto assets EU 2023/1114) and being subject to the obligations of the Travel Rule under the TFR Recast.[34]

The TFR recast introduced **enhanced anti-money laundering (AML) and counter-terrorist financing (CTF) requirements** for **crypto-asset service providers ('CASPs')** operating within the European Union. The regulation aims to *inter alia* improve the **traceability of transfers of funds and crypto-assets** and reduce financial crime.

One of the aspects emerging in this Complaint is the impact of the Travel Rule, as a measure to protect against money laundering and the financing of terrorism, and the protection offered to the consumer who fell victim to fraud, which fraud it was claimed could have been avoided if the CASP had honoured its obligation under the Travel Rule properly.

There is no doubt that the Travel Rule has as its main objective the prevention and detection of money laundering and terrorism financing (AML/CTF). The new obligations constitute an important part of the financial services legislative framework to which CASPs are now subject.

[32] P. 29 - 41 & 53
[33] P. 122 - 132
[34] The Service Provider's VFA licence was surrendered on 27 January 2025, with the MiCA license issued on the same day and thus after the disputed transactions.

Consideration thus needs to be given to these new responsibilities, taking into account the fiduciary and duty of care obligations and the requirement to act in the best interests of clients, as applicable to the Service Provider with respect to the financial services it offered to the Complainant as its customer.

The Arbiter will consider whether, in this particular case, the Service Provider has honoured its obligation under the Travel Rule, and if not, whether any failure to do so has prejudiced the Complainant's interests, leading him to incur the losses he is trying to recuperate through this Complaint.

This consideration will determine whether the alleged failure of a regulatory obligation gives rise to any liability on the financial service provider, if it is proven that the failure of the regulatory obligation harmed the client's interests and gave rise to a lack of due skill and care owed towards the client.

Defence raised with reference to AML/ CFT and other relevant matters

It is noted that as part of its defence, the Service Provider raised the point that *'the Arbiter is not the competent authority to adjudicate or hear allegations relating to AML and CFT matters as these should be dealt with by the FIAU in accordance with Chapter 272 of the Laws of Malta'*.[35]

The Arbiter fully concurs that he is not the competent authority to investigate and adjudicate failures related to ML/FT issues, as these undoubtedly fall within the remit of the FIAU. It is indeed the FIAU that has the enforcement powers to impose administrative penalties and take other measures permitted by law against subject persons in respect of any breach of AML and CFT obligations.

For the avoidance of doubt, the Arbiter is accordingly not considering or assessing whether there was, or should have been, any suspicion of money laundering activities or operations related to the financing of terrorism in the consideration of this Complaint.

The Arbiter's consideration is limited to, and only focuses on, determining whether any material implications arise to the Complainant's detriment and the losses he incurred as a result of a failure of the regulatory obligation (in this case the Travel Rule) to which the Service Provider is subject.

[35] As argued by the Service provider p.148 para. 26

As outlined above, such an obligation forms part of the financial legislative framework which binds the conduct of the financial service provider in respect of the financial services it has offered to its customers.

It is indeed within the competence of the Arbiter to investigate and adjudicate whether the claimed non-adherence with the Travel Rule obligations has prejudiced or otherwise the interest of a financial consumer who is a client of the Service Provider and whether any such failure caused and contributed to the losses suffered, as the Complainant is arguing in this Complaint. As also outlined above, **the Arbiter shall focus his considerations on this aspect taking into account the fiduciary and duty of care and conduct obligations applicable to the Company as a financial services provider.**

There is no doubt that by virtue of its role and functions, the Service Provider has a fiduciary duty and duty of care towards its customers.[36] The fiduciary duty was also acknowledged in a recent decision issued by the Court of Appeal involving the same provider and the nature of services provided[37] where it was *inter alia* noted that:

> *'Din il-Qorti tibda billi tqis li l-Arbitru korrettament kkonstata li s-soċjetà appellata kellha obbligazzjonijiet ta' natura fiduċjarja …'.* [38]

As a VFA Service Provider under the VFA regime, the Company was also subject to various conduct of business obligations, requiring it, *inter alia*, to act in the

[36] E.g. Article 27 (*Fiduciary Obligations*) of the VFA Act pointed out that: *'27. (1) Licence holders shall act honestly, fairly and professionally and shall comply with the requirements laid down in this Act and any regulations made and rules issued thereunder, as well as with other legal and regulatory requirements as may be applicable. (2) A licence holder shall be subject to fiduciary obligations as established in the Civil Code, in so far as applicable.'*

[37] The exchange of fiat into crypto and the transfer of crypto-assets to other wallets.

[38] Para. 12 page 36 of the Court of Appeal (Inferior Jurisdiction) No. 35/2025 LM.

best interests of clients.[39] It remained similarly subject to the same principles and requirements under the MiCA regime.[40]

Other aspects

The specific circumstances of this Complaint show that at the time of executing the disputed transfers the Service Provider had no alert flagged internally by its systems that the recipient wallets, which later were claimed to be fraudulent, were linked to any fraudulent activity.

The Arbiter notes that the Service Provider thus claimed that the transfers had no out-of-ordinary characteristics which could have triggered the need for it to investigate before proceeding with the execution of the transfers.

In the circumstances, the Arbiter must consider whether the Service Provider has complied with the requirements of the Travel Rule by taking adequate measures to satisfy themselves that the recipient external wallet was truly owned or controlled by the Complainant as he had explicitly declared.

Service Provider's obligations under the EBA Travel Rule Guidelines

At the time of the disputed transactions, the Service Provider was subject to the *'Guidelines on information requirements in relation to transfers of funds and certain crypto-assets transfers under Regulation (EU) 2023/1113'*, Final Report

[39] For example, the High-Level Principles in Chapter 3 of the Virtual Assets Rulebook, Virtual Financial Assets Rules for VFA Service Providers issued by the MFSA under the VFA Act provided that: *'R3-1.2.1 VFA Service Providers shall act in an ethical manner taking into consideration the best interests of their clients and the integrity of Malta's financial system.*

R3-1.2.2 VFA Service Providers shall act honestly, fairly and professionally in accordance with the best interest of clients and prospective clients and shall comply with the relevant provisions of the Act, the VFA Regulations issued thereunder, and these Rules as well as with other relevant legal and regulatory requirements.'
…

R3-3.4.3.10.3 The Licence Holder shall not, in any communication or agreement with a Client (except where permitted by applicable legislation), exclude or restrict, or seek to exclude or restrict:
i. any legal liability or duty of care to a Client which it has under applicable law or under these Rules;
ii. any other duty to act with skill, care and diligence which is owed to a Client in connection with the provision to that Client of a virtual financial asset or VFA Service; or
iii. any liability owed to a Client for failure to exercise the degree of skill, care and diligence that may reasonably be expected of it in the provision of a virtual financial asset or VFA Service.'

[40] For example, Recital (79) of Regulation (EU) 2023/1114 (MiCA), provides that *'In order to ensure consumer protection, market integrity and financial stability, crypto-asset service providers should always act honestly, fairly and professionally and in the best interests of their clients.'* Article 66(1) of MiCA further stipulates the obligation for all CASPs to act honestly, fairly and professionally in the best interests of clients.

(EBA/GL/2024/11) issued by the European Banking Authority ('EBA') in July 2024[41] ('the Travel Rule Guidelines' or 'Guidelines').

The said Guidelines need to be referred to by competent authorities:

> *'when assessing whether the procedures PSPs, IPSPs, CASPs and ICASPs have put in place to comply with Regulation (EU) 2023/1113, are adequate and effective'.* [42]

The Travel Rule Guidelines were adopted by FIAU, with effect from 30 December 2024, in terms of Regulation 17 of the Prevention of Money Laundering and Funding of Terrorism Regulations as outlined in the public notice dated December 2024 issued by the FIAU.[43]

It is noted that in its final submissions, the Service Provider refers to para. 78 of the Guidelines which states as follows:

> *'If such information[44] cannot be retrieved via technical means, the originator's CASP and the beneficiary's CASP should obtain that information directly from its customer …'.*

The Service Provider maintains that it abided with this obligation as it took measures to obtain a signed declaration from the Complainant that he was the owner of the recipient external wallet.

This was done by ticking a box in its systems which declared:

> ***'I am the owner of this wallet address'***

with the Complainant then giving the wallet address and declaring that it is a non-custodial wallet (meaning that it is a self-hosted external wallet NOT under the control of a licensed CASP with whom the Service Provider could make additional verifications).

[41] https://www.eba.europa.eu/sites/default/files/2024-07/6de6e9b9-0ed9-49cd-985d-c0834b5b4356/Travel%20Rule%20Guidelines.pdf
[42] *Ibid.*
[43] https://fiaumalta.org/app/uploads/2024/12/Dec-2024-Travel-Rule-Guidelines.pdf
[44] Per para. 77 of the Guidelines, being information necessary to determine whether or not a recipient wallet is a self-hosted wallet (external wallet)

There is a warning that:

> ***'If the user ticks the box to indicate they are the owner of the wallet address, they will be required to provide the 'Wallet Type' and the 'Wallet Name' before they can proceed with whitelisting'.***[45]

In this particular case, the Complainant ticked the box[46] declaring he is the owner of the wallet address and, also, declared that the wallet type was non-custodial but did not quote any wallet name. Despite giving no name and just relying on the Complainant's self-declaration without verification, the wallet was white-listed and transfers to such external self-hosted wallets were allowed after the usual notices were given to the Complainant.

The Arbiter, however, takes into consideration paras. 83 - 86 of the Guidelines which further state as follows:

> ***'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.'***

This clearly shows that the CASP was required to go beyond the Complainant's self-declaration of ownership and make its own and further verifications.

The verifications included in para 83 of the Guidelines as applicable to this case are:

> *'a) unattended verifications as specified in the Guidelines on the use of Remote Customer Onboarding Solutions under Article 13(1) of Directive (EU) 2015/8499 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 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;*

[45] P. 135
[46] *Ibid*.

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;'

The Guidelines further provide as follows:

'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;

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 and 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 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 the address from its whitelist.'

No evidence was submitted by the Service Provider that it took any of the verification methods requested by the Guidelines.

During the hearing of 04 December 2025, there is recorded as follows:

'The Arbiter states that, if he understands correctly, these transfers to these wallets, which later turned out to be fraudulent wallets, [the Complainant] ticked the box where he confirmed that he was the owner of these wallets.

> ***And that, according to the Service Provider, this is sufficient defence that by accepting that declaration, you satisfy the Travel Rule obligations which we know about, that you have to take certain action that these were transferred to a known beneficiary of the receiving wallet.***
>
> ***Asked by the Arbiter whether this is correct, [the Service Provider] confirms that this is correct.'*** [47]

The Arbiter is of the firm opinion that the Service Provider had obligations under the Travel Rule to make further verification and not simply rely on the Complainant's self-declaration.

Reference is also made to the term '**fully satisfied'** in Para. 83(e) and 86 of the Guidelines. It is argued that no CASP can achieve a degree of being **'fully satisfied'** if it merely relies on a simple self-declaration of the Complainant through a tick-box method.

Requested Policies & Procedures

It is noted that Guidelines 12 and 14, Section 4.1, General Provisions of the Travel Rule Guidelines, require CASPs to document how they will ensure compliance with the TFR Recast:

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

[47] P. 139

By way of a decree dated 7 January 2026, the Arbiter requested the Service Provider (apart from other parties) to produce the following documentation:

(i) a copy of the policies and procedures required under the EBA's Travel Rule Guidelines[48] that were originally put in place by the Service Provider to ensure compliance with the indicated Guidelines from the date of their application, 30 December 2024, with respect to the transfer of crypto-assets;

(ii) a copy of any, and each, subsequent version (clearly dated) of such policies and procedures issued since, with any updates and changes thereto.

Despite the Arbiter's specific request that was made in terms of Article 25(5) of Cap. 555, **the Service Provider failed to produce a copy of its internal policies and procedures document**.

In its note of 29 January 2026, the Service Provider only limited itself to providing just the following:[49]

a) a post from its website titled *'European Union – Travel Rule Requirements FAQ'*;[50]

b) screenshots of the wallet address whitelist process as was currently in effect at the date of its note;

c) a blank Travel Rule declaration form.

The above were mainly already provided as attachments to its final note of submissions of 9 January 2026.

A reproduction of a post from its website and just a copy of the forms a user was required to complete on its systems are considered rather inadequate and weak attempts to demonstrate the required documented policies and procedures. Properly documented steps of how compliance is ensured with the TFR Recast

[48] EBA Guidelines on information requirements in relation to transfers of funds and certain crypto-assets transfers under Regulation (EU) 2023/1113 ('Travel Rule Guidelines') of 4 July 2024 (EBA/GL/2024/11)
[49] P. 164 -174
[50] https://help.crypto.com/en/articles/10190809-european-union-travel-rule-requirements-faq

would be expected and should rather emerge from the Company's own properly documented and dated internal policies and procedures manual.

In addition, from the information provided, the Arbiter could not reasonably conclude that the Service Provider's procedures reflect and satisfy all the relevant requirements stipulated under the TFR Recast and Guidelines. This is particularly so with respect to the assessment and verification required related to the proof of ownership or controllership of a self-hosted address in terms of Guidelines 83 to 86 of the Travel Rule Guidelines.

The above conclusions are reached on the basis that:

(i) not only are such specific provisions of the Guidelines not adequately covered nor reflected in the information outlined above that were provided to the Arbiter by the Service Provider, but

(ii) also, no evidence has been produced that the Service Provider in practice undertook any such assessment and verification using the methods stipulated in the said Guidelines.

The FAQ document provided outlines that *'If the withdrawal amount is over 1,000 EUR and the beneficiary party is a non-custodial wallet, you may be required to provide additional information'*.[51]

In the case of a transfer above EUR 1,000 to a self-hosted address (that is, a non-custodial wallet), it is not optional but mandatory for assessment and verification to be conducted unless already whitelisted previously.

Furthermore, the FAQ document and forms provided do not even mention or delve into the method(s) of how/when the Service Provider will undertake the required assessment and verification using the verification methods outlined in the Guidelines. This is a key omission emerging from the information provided and, also, reflected in practice in the actions, or lack thereof, of the Service Provider.

No adequate proof has indeed been provided that the Service Provider has documented in its systems that it had *'fully satisfied that the self-hosted address*

[51] P. 167

is owned or controlled by its customer', as was required in terms of the said Guidelines as outlined earlier above.

It is also noted that in one of the forms related to the whitelisting of an external wallet, the Service Provider outlines that:

> *'If the user ticks the box to indicate they are the owner of the wallet address, they will be required to provide the 'Wallet Type' and 'Wallet Name' before they can proceed with whitelisting'*.[52]

Again, the form omits further details about the assessment and verification method(s) to enable the Service Provider to be fully satisfied that it knows who owns or controls the external wallet address.

Other Considerations – Industry Practices

In its testimony during the hearing of 4 December 2025, the Service Provider explained that the Complainant ticking *'the box where he confirmed that he was the owner of these wallets … is sufficient defence'* of satisfaction of the Travel Rule obligations.[53]

The Arbiter considers that compliance with the Travel Rule requirements is, however, not just a box-ticking exercise nor that such self-declaration form was sufficient or reflective of the applicable requirements. It is deemed that compliance with the Travel Rule obligations rather entails an active assessment undertaken on the part of the CASP using the specified verification methods outlined in the Travel Rule Guidelines.

It is again highlighted that when it comes to proof of ownership or controllership of a self-hosted address (in the case of transfers above Eur1,000), the Service Provider had to not just be merely satisfied but the requirements required of it to be ***'fully satisfied',*** with the Guidelines listing the type of verification methods.

The Arbiter notes that another local CASP, which had been similarly requested to provide a copy of its policies and procedures, listed in its internal operational

[52] P. 172
[53] P. 139

document three authorised methods[54] for the purpose of whitelisting and confirmation of the wallet control and ownership, namely, as follows:

(i) the Satoshi Test (on-chain verification)[55]

(ii) the Digital Signature Verification (off-chain proof of ownership)

(iii) the Screen Video record confirmation (as a fall back procedure).

It is noted that one or more of the above verification methods are seemingly commonly applied and used by other CASPs.[56]

Further Analysis and Concluding Remarks

Recital 39 of the TFR Recast provides that:

'(39) In the case of a transfer to or from a self-hosted address, the crypto-asset service provider should collect the information on both the originator and the beneficiary, usually from its client. A crypto-asset service provider should in principle not be required to verify the information on the user of the self-hosted address. Nonetheless, ***in the case of a transfer of an amount exceeding EUR 1 000 that is sent or received on behalf of a client of a crypto-asset service provider to or from a self-hosted address, that crypto-asset service provider should verify whether that self-hosted address is effectively owned or controlled by that client.'***[57]

Article 14 of the TFR Recast, which deals with the *'Obligations on the crypto-asset service provider of the originator'* is particularly relevant and applicable to the Service Provider as the CASP of the Complainant (the originator).[58]

As outlined in Article 14(5),

[54] Seemingly to address the verification methods outlined in EBA Guideline 83, namely 83(c), (d) and (e).
[55] The Satoshi Test is a verification method used to verify control of a self-hosted wallet. https://www.okx.com/en-eu/help/whats-satoshi-test-and-how-do-i-complete-it
[56] https://www.binance.com/en/support/faq/detail/0144ac061746409fae64a2166a214fa4 https://support.kraken.com/articles/what-is-a-satoshi-test https://www.etoro.com/crypto/travel-rule/
[57] Emphasis added by the Arbiter
[58] Article 3(21) of the TFR Recast defines 'originator' to mean *'a person that holds a crypto-asset account with a crypto-asset service provider, a distributed ledger address or a device allowing the storage of crypto-assets, and allows a transfer of crypto-assets from that account, distributed ledger address, or device, or, where there is no such account, distributed ledger address, or device, a person that orders or initiates a transfer of crypto-assets'*

'… in the case of a transfer of an amount exceeding EUR 1000 to a self-hosted address, the crypto-asset service provider of the originator ***shall take adequate measures to assess whether that address is owned or controlled by the originator'.***[59]

The adequate measures required from the respective CASP (that is, the CASP of the originator and the CASP of the beneficiary) are then further elaborated on in Section 4.8 of the EBA's Travel Rule Guidelines, titled *'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'*).

The Service Provider's role in terms of the Travel Rule was not just limited to obtaining and maintaining the information disclosed by the consumer in its forms about the external wallet, nor in just ensuring that the external wallets were not labelled as suspected in its transaction monitoring system, as testified during the hearing of 4 December 2025.

Its obligations went beyond as it had a key obligation to also assess and verify using at least one of the listed verification methods whether the self-hosted address is owned or controlled by the originator as outlined in section 4.8.4 of the Travel Rule Guidelines. The effectiveness of just relying on a self-declaration is questionable to the point that on its own does not provide a robust and adequate assessment.

The defence made by the Service Provider with reference to paragraph 78 of the Travel Rule that the originator's CASP should obtain information *'directly from its customer'* does not justify or excuse the Service Provider from not undertaking the assessment and verification (through the verification methods) outlined in paragraph 83 of the Travel Rule Guidelines as outlined above. A mere tick-the-box confirmation by the Complainant that he was the owner of the external wallet address was clearly not sufficient and did not reflect and address the specific verification methods that the Service Provider was obliged to undertake under the EBA's Travel Rule Guidelines for the purpose of the assessment required under Article 14(5) of the TFR Recast.

[59] Emphasis added by the Arbiter

The Arbiter accordingly does not share the Service Provider's opinion that *'it was under no obligation to raise additional questions where the customer unequivocally identified himself as the wallet owner'*.[60]

In its final submissions, the Service Provider additionally referred to Article 16(2) of the TFR Recast. This article relates to the obligations of the CASP of the beneficiary (and hence not the Service Provider) and, accordingly, does not justify either the lack of assessment and verification that was required by the CASP of the originator (that is, the Service Provider) in terms of Article 14(5) and the Travel Rule Guidelines.

Having concluded that the Service Provider failed its obligations under the Travel Rule, the Arbiter proceeds to consider whether this failure was a cause of the loss suffered by the Complainant, subject of this complaint, in part or in full.

Causal Factor

The Arbiter is of the opinion that had the Service Provider proceeded to perform additional verification(s) as demanded by the Guidelines, there would have been a fair probability that it would transpire that, contrary to what was indicated, the self-hosted external wallet was not under the ownership or controllership of the Complainant.

The degree of such probability may be a subjective judgement, and the Arbiter has also to take into consideration that a substantial contributory cause of the loss is the negligence of the Complainant in not taking adequate precautions to avoid the fraud and making, knowingly or unknowingly, and under the guidance of the scammers, false declaration of ownership.

The Arbiter considers that there is nevertheless a clear link between the identified failures of the Service Provider and the losses sustained by the Complainant. If the Service Provider had properly carried out its duties, it would have likely realised that, contrary to what was claimed, the Complainant did not own or control the external wallet address to which the disputed transfers were undertaken. This would then have triggered the need for the Service Provider to freeze or suspend the transfers; seek the appropriate clarifications and prohibit the transactions. No such actions were, however, undertaken with the transfers

[60] P. 151

processed without question, enabling easy access to the funds for the fraudsters.

As outlined above, consideration also needs to be taken of the negligence arising on the Complainant's part. This is particularly when considering the apparent lack of checks by the Complainant about the legitimacy of the platform *9bxz.com*; the incorrect disclosures the Complainant himself made that he was the owner/ controller of the external wallet; the Complainant proceeding with the transfers despite the warning about external wallets provided by the Service Provider;[61] and also given that the Complainant kept interacting and following the instructions of the scammer notwithstanding that he was already suspecting fraud.

Other Considerations - Higher Expectations from CASPs

The Arbiter points out that, given the extent of sophisticated scams and fraud that have been disturbingly emerging globally, both he and his predecessor have issued multiple decisions throughout the past years (since late 2022),[62] strongly urging CASPs to take enhanced measures and actively work to mitigate the occurrence of customers falling victim of scams.

In the context where:

- there is now a regulatory framework which is aimed to '*prevent terrorists, money launderers, proliferation financiers and other criminals (e.g., fraudsters) from accessing wire transfers to move their funds …'*,[63] and whose '*main objective is to make the abuse of funds and certain crypto-asset transfers for terrorist financing and other financial crime purposes more difficult'*,[64] and

[61] P. 154
[62] Example – Case ASF 158/2021 decided in December 2022, and Case ASF 069/2024 decided in September 2024: https://financialarbiter.org.mt/sites/default/files/oafs/decisions/457/ASF%20158-2021%20-%20AG%20vs%20Foris%20DAX%20MT%20Limited.pdf
https://financialarbiter.org.mt/sites/default/files/oafs/decisions/1912/ASF%20069-2024%20-%20UP%20vs%20Foris%20DAX%20MT%20Limited.pdf
[63] Page 4 of the FATF, Best Practices, Travel Rule Supervision, June 2025: https://www.fatf-gafi.org/content/dam/fatf-gafi/recommendations/Best-Practices-Travel-Rule-Supervision.pdf
[64] Page 3 of EBA's Final Report (EBA/GL/2024/11]

- the specific obligations placed upon CASPs with respect to transfers to self-hosted wallets of over Eur1,000 as applicable under the said regulatory framework (TFR Recast and Travel Rule Guidelines) as considered above;

- the direction that the Service Provider has been receiving from the Arbiter's decisions over the past years preceding the disputed transactions, with regard to its role in protecting consumers;

- the gravity of the failure to verify the owner/controller in respect of the second transfer is compounded due to the Service Provider having overlooked and ignored the *Report of Loss*.

  The Complainant submitted that he reported his particular case on 2 January 2025 (before the second transfer of 16 January 2025). The Complainant's consistent claims of such report[65] was not actually contested by the Service Provider.

  Despite his reporting that he had lost funds, no evidence has emerged that the Service Provider has internally flagged the Complainant's account and marked the client as a potential victim of a scam for enhanced monitoring, as would reasonably have been expected in the circumstances. This should have heightened his risk classification and the need for increased alertness on his account in view of his vulnerability.

  It would have been proper and in the best interests of the client had the Service Provider suspended further transactions and/or first sought further clarifications prior to proceeding in accepting additional new transfers to external non-custodial wallets and this when transfers to a self-hosted wallet have heightened risks as compared to a transfer to a custodial wallet. This adds to the gravity of its actions of just relying on an unverified self-declaration by a vulnerable client, and its failure to verify the owner/ controller of the external wallet as required in terms of the Travel Rule Guidelines;

[65] As claimed in his Complaint Form (P. 3, 21); Formal complaint with the Service Provider (P. 7); Extract of interaction with the Company's Customer Support (P. 52) and again during his testimony of 17th June 2025 (P. 107)

the Arbiter finds the Service Provider to have failed in its fiduciary and duty of care obligations and to act in the best interests of its client as was reasonably expected of it, and to also meet the reasonable and legitimate expectations of its client.

The latter is an aspect that the Arbiter is *inter alia* also obliged to consider and have due regard to in terms of Article 19(3)(c) of the Act.

Decision

The Arbiter is obliged by Article 19(3)(b) of CAP. 555 of the Laws of Malta to determine and adjudge a complaint by reference to what, in his opinion, is fair, equitable and reasonable in the particular circumstances and substantive merits of the case.

In the circumstances, and given the respective shortcomings, the Arbiter is only partially upholding the request for compensation for the suffered loss. The Arbiter considers that the Complainant must shoulder a major part of the loss resulting from his contributory negligence as above explained. No compensation for additional moral damages as requested by the Complainant will be awarded.

For the reasons amply explained above the Arbiter is upholding this Complaint to a limited extent and in terms of Art. 26(3)(c)(iv) of CAP. 555 of the Laws of Malta is ordering the Service Provider to pay the Complainant €12,000 (twelve thousand euros) being 40% of the loss suffered by the Complainant through the transfers subject matter of this Complaint.

With interest at the rate of 2.15% p.a.[66] from the date of this decision till the date of payment.[67]

Each party is to bear its own legal costs of these proceedings.

[66] Equivalent to the current Main Refinancing Operations (MRO) interest rate set by the European Central Bank.
[67] It is to be noted that in case this decision is appealed, should this decision be confirmed on appeal, the interest is to be calculated from the date of this decision.

This decision is being brought to the attention of MFSA (Malta Financial Services Authority) and FIAU (Financial Intelligence Analysis Unit) it being the first of its kind since the Travel Rule regulation came into effect.

Alfred Mifsud
Arbiter for Financial Services

Information Note related to the Arbiter's decision

Right of Appeal

The Arbiter's Decision is legally binding on the parties, subject only to the right of an appeal regulated by article 27 of the Arbiter for Financial Services Act (Cap. 555) ('the Act') to the Court of Appeal (Inferior Jurisdiction), not later than twenty (20) days from the date of notification of the Decision or, in the event of a request for clarification or correction of the Decision requested in terms of article 26(4) of the Act, from the date of notification of such interpretation or clarification or correction as provided for under article 27(3) of the Act.

Any requests for clarification of the award or requests to correct any errors in computation or clerical or typographical or similar errors requested in terms of article 26(4) of the Act, are to be filed with the Arbiter, with a copy to the other party, within fifteen (15) days from notification of the Decision in terms of the said article.

In accordance with established practice, the Arbiter's Decision will be uploaded on the OAFS website. Personal details of the Complainant(s) will be anonymised in terms of article 11(1)(f) of the Act.