Before the Arbiter for Financial Services

Case ASF 186/2025

ZO

('the Complainant')

vs

Foris DAX MT Limited

(Reg. No. C 88392)

('Foris', 'the Company' or 'Service Provider')

Sitting of 15 May 2026

The Arbiter,

Having seen the Complaint[1] made against Foris DAX MT Limited relating to its alleged failure to stop the execution of four transfers of digital assets to two fraudulent externals wallet involving a self-hosted address.[2]

The Complainant argues that his authority for making these transfers was technically correct but his authority was vitiated by psychological pressure and manipulation by fraudsters.[3]

From the reply of the Service Provider, it appears that these transfers were funded and executed as follows:

[1] Pages (p.) 1- 12 and attachments p. 13 - 178

[2] 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'*

[3] P. 3

DATE	Transfer in €	Converted to USDC/USDT	Transferred out USDC/USDT	Ref
01.01.2025	1,708	1741.53	1731.36	p. 187
06.01.2025	4,050	4139.81	4129.97	p. 188
13.01.2025	3,005	2967.86	2957.86	p. 189
03.02.2025	2,400	2417.93	2407.93	p. 190
TOTAL	**11,163**	**11267.13**	**11227.12**	

These four transfers amounting to €11,163 were immediately converted to USDC or USDT[4] and promptly transferred to 2 external (self-hosted) wallets with codes ending ….3338B and ….foC97.

The Complainant is demanding reimbursement of 70% of his loss and is requesting the Arbiter to grant him compensation of €7,841 acknowledging his partial contribution to the scam event through negligence.

He claims that Foris are responsible for 70% of his loss due to:

- Failure of duty of vigilance citing European Anti-Money Laundering (AML) Directive and Know your Customer (KYC) rules.
- Incorrect email address communicated by Crypto.com (brand name of Foris) which led to delay in his lawyer's investigation to trace his stolen funds and compromised his chances of recovery.
- Lack of assistance and resistance to provision of necessary information which increased stress caused by the loss.

[4] USDC and USDT as digital stable coins having market value at par 1:1 with USD.

Reply of Service Provider[5]

In their Reply, the Service provider gave the following background:

1. *"Background*

- *Foris DAX MT Limited (the '**Company'**) offers the following services: a crypto custodial 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.*
- *Our Company 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.*
- *(The Complainant), e-mail address xxxxx@gmail.com, became a customer of Foris DAX MT Limited through the Crypto.com App and was approved to use the Wallet on 8 December 2024.*
- *The Company notes that in the submitted complaints file, the Complainant's representative has outlined the desired remedy as: (i) reimbursement for incurred financial losses*."[6]

Then they gave a timeline of the activity on the Complainant's account and concluded as follows:

"Based on our investigation, the Company has concluded that we are unable to honor the Complainant's refund request based on the fact that the reported transfers were made by the Complainant himself.

While we sympathize with the Complainant and recognize 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. We must also emphasize that the addresses the funds were transferred

[5] P. 186 - 193 and attachments p. 194 - 201
[6] P. 186

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 said wallets.

Unfortunately, Crypto.com cannot revoke any virtual asset withdrawals because blockchain transactions are fast and immutable.

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 and Conditions.

Please see the relevant section of the Terms & Conditions for your reference:

'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.

…'

The Crypto.com App Terms and Conditions are and have always been available to the Complainant from within the Crypto.com App under the Settings – About tab.

Service Provider's Warnings

In the course of the Complainant's Disputed Transactions, the Service Provider would have provided numerous warnings regarding withdrawals to non-custodial wallets.

The first of these warnings appear whenever a user adds a new withdrawal address to the Cryto.com App. For the reference of the Tribunal, the warning appears as below, in Fig. 13. This warning invariably appears whenever the adding of a new withdrawal address, known as "Whitelisting" occurs, and takes the form of a full screen pop-up.

A similar warning appears at the time of each withdrawal, whether or not the withdrawal address is newly whitelisted or to a withdrawal address which has already been whitelisted on a previous occasion. An example of this warning can be found below, exhibited as Fig. 14.

As can be seen from the examples provided below, both pop-up warnings specifically warned the Complainant against scams and not to whitelist or withdraw digital assets to 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 warning displayed during withdrawals, the Complainant is further warned that the withdrawal is 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 Center page "Avoiding Digital Currency Scams" (a screenshot of the current page https://help-

crypto.com/en/articles/6484926-avoiding-digital-currency-scams is labelled Fig. 15 in the Appendix).

Upon the Complainant confirming that they had read the scam warning by clicking on the "Confirm and Withdraw" button on the pop-up warning, the Complainant confirmed they accepted the risks involved and took full responsibility for the withdrawals to the External Wallets, specifically agreeing to and acknowledging that the withdrawals were irreversible and that the Service Provider would not be liable for assets sent to the External Wallets.

In spite of the numerous warnings mentioned above, the Complainant proceeded to make the withdrawals to the External Wallets. It can be seen that the Complainant either negligently disregarded the warnings, or was otherwise unaffected by them.

Summary

In summary, 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 Foris DAX MT, we can neither confirm nor deny this.

Whilst we fully empathize 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.

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."[7]

Hearings

A first hearing was held of 27 November 2025, for the evidence of the Complainant where he stated:

[7] P. 191 - 193

“I say, yes, absolutely. I speak about my experience. Yes, I was victim of a boiler room type of fraud. And those frauds are known for psychological manipulations, pressure on the victims.

The Arbiter states that what he would like to establish is that when I was making these payments, obviously I was not aware of the fraud and that all these payments were made under my authority.

I say not 100% because when someone exerts psychological manipulation, pressure, it's not me, my free will was affected.

The Arbiter says that at this point in time, he is asking me to confirm that these payments were made by me and not by somebody who stole my credentials and made the payments without my knowledge.

I say that the payments were made by me. I explained that in my complaint.

I am asked by the Arbiter to explain why I think that Crypto.com should make a contribution of 70% to my losses.

I say I thought that because I was confused by the information provided by Crypto.com. And this confusion caused a loss of time. With this confusion, with providing the wrong address email by Crypto.com and with the loss of time, I was victim of that. It resulted in the loss of my lawyer, and my lawyer was my only support and help in this case.

I consider that if I had the correct information in time, we had a chance to have to block the cryptocurrency wallet of the scammers. Why? Because I searched after that where my money went. And with my research, I found that they went to a cryptocurrency wallet that belonged to Pulsar LTRB and Pulsar LTRB is supervised by the Great Bank of Lithuania. It's a FinTech of Lithuania. My lawyer has experience enough because he has a case similar to mine and he has experience enough to contact the Great Bank of Lithuania because he made this in the past. And then I said, but if we had the correct information in good time, it was possible for my lawyer to contact the authority to create a channel of communication between the authorities in Belgium and the Great Bank of Lithuania. But, with the loss of time, we lost a chance here, we lost the opportunity here to do anything. I discovered that too late. I contacted the

authorities too late and the loss of time is responsible for this lack of responsibility.

The Arbiter states that if he understands correctly, to put it in a nutshell, what I am saying is that once I was aware that I had been scammed, there are two issues for which I am accusing Crypto.com. One is bad service because they did not reply in time, they gave me some wrong information, et cetera, and the other one is that as a result of this bad service, there was a delay in my ability to make the necessary investigations to try to block the funds, and that contributed to the loss.

I agree that this is the correct interpretation of what I said."[8]

Under cross examination, he stated:

"It is being said that in my complaint, I say that, 'I was subjected to an attempt to modify my personal information on Crypto.com account. Indeed, someone tried to change my phone number. Despite the alert I received, I was given no information about the identity of the person who initiated it'.

Asked whether I received an alert that someone was trying to change information from my Crypto.com account, I say, yes.

Asked whether this means that my phone or my account was hacked at the time, I say, I do not know. I asked Crypto.com to give me some information, but Crypto.com told me that it was confidential, and I can understand it, but it was very difficult for me to accept this because I was victim of scam.

It is being said that what I am saying is that I asked Crypto.com to give me evidence or to tell me who had initiated this change and who was trying to change my account information. Asked if it wasn't me trying to change this information does this mean that someone else was obviously trying to change this information, I say, yes, absolutely.

It is said that when someone was trying to change the information from my account, and it was not done by me, I received an alert from someone telling me that my account information is trying to be changed.

[8] P. 203 - 205

I say I was not alerted by someone, but by Crypto.com.

It is said that I received an alert telling me that someone is trying to change my Crypto.com account information.

I say, no, not exactly. I received an alert here from Crypto.com and they asked me if I am responsible for changing my number, my phone number. And then I said, no, it's not me.

It is said that then, I asked and then they told me that they could not give me this information. And if it weren't me, it was someone else then who was trying to change this information.

Asked whether my phone account was hacked or whether I shared my Crypto.com login access details, etc., with the scammers, whether I had given them access to my account, I say, no.

Asked whether I had given them access to my device, I say, no. Absolutely not, no. I participated in their system only to have benefits. I don't share everything with everyone. No, I didn't do that.

Asked whether I had any other sharing device or app which they told me to install on my phone, I say, no.

Asked whether they told me to install anything like AnyDesk or Share or something like that, I say no, because the day I participated in the system, I made it from another computer, not mine; and I did not share anything with them.

Asked whether I accessed my Crypto.com in there, I say, no.

Asked whether my phone or my laptop was acting as though it was compromised at the time if this was not me trying to change this information; and asked who had access to my account and whether there was anyone else who had access to my account, I say, no one else. No one else.

That was very strange for me because I know that Crypto.com is a big company. They have tools to protect consumers. I know, but I didn't understand then why that appears. I don't have expectations really because I don't share everything with everyone.

The Arbiter would like to clarify whether this attempt to change the telephone number happened after the scam, not before the scam.

I say, yes, after the scam. I was the victim of the scam in the month of February, and that appears in the month of April 2025.

It is said that I am insisting and saying that I had no redress because my lawyer decided that he was not going to represent me because of the delay or whatever. However, the information I needed was my address, my Crypto.com account number, and the external wallet address to which I sent the money. That is the information that I required. There was no other information that Crypto.com had to give me which I did not already have.

Asked whether I agree, I say, yes.

It is said that in my reply, I also mentioned the lack of AML monitoring procedures, etc., (page 7 of my complaint), where I say that these repetitive transactions should have triggered AML protocols within the system.

Asked whether it had not been made clear on several occasions that the disclosure of these protocols is not allowed on the basis of the fact that it is against AML regulations to let everyone know what Crypto.com's protocols are, I say that I am not an expert in what the AML rules are, but what can I say? I made then four transactions, the first at the beginning of the month of January 2025, and the last on 3 February 2025.

I am asked whether, when making all these transactions, I recall receiving all the warnings which Crypto.com said they sent me in their reply to this complaint; whether I remember receiving a pop-up warning on several occasions before I made these transactions.

I say that this is the problem. I do not remember that there was anything here. I transferred this money easily, simply.

The Arbiter explains what Crypto.com said that whenever I make a payment, they flash up to me a warning to be careful. Asked whether I remember seeing

this warning before I made each payment, I say I do not remember. I tried, but I really do not remember." [9]

At the second hearing held on 30 January 2026, the evidence of Foris was provided by Pema Fung who stated:

"The complainant became a client and user of the service provider on the 8th of December, 2024.

The disputed transactions in question relate to four withdrawals of cryptocurrency, which were purchased in the complainant's crypto.com app account and sent to two external wallet addresses between the 2nd of January and the 3rd of February, 2025.

These wallet addresses are what we call non-custodial addresses, which means they are not serviced by Crypto.com, or identified from data on the blockchain provided as serviced by other service providers of hosted exchanges.

With regards to the wallet addresses which the withdrawals were made to, as these were new wallet addresses, these addresses would have had to pass through the whitelisting process. Firstly, the complainant would have had to complete the Travel Rule form which asked him to indicate whether the external wallet to which funds were being transferred was self-hosted or otherwise, and also 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 distributed ledger address or wallet address, and the unique transaction identifier of the wallet.

Each transfer initiated by the complainant could therefore be individually identified. In this particular case, the complainant had indicated that the two wallets were self-hosted and owned and controlled by himself, and this was confirmed via a form submitted by him. The same declaration was made for all transfers.

[9] P. 205 - 207

The complainant was provided with clear instructions on how to complete the Travel Rule form, and this Travel Rule form was drafted by our internal compliance team and is considered to be compliant with the Travel Rule. This information was collected, and scam warnings were given with each withdrawal and whitelisting processed. This evidence was filed earlier today with the complainant being copied in the email.

With regards to these warnings, in the course of the complainant's disputed transactions or withdrawals, the service provider had numerous warnings provided regarding withdrawals to the external wallets which have been detailed in the filed document.

The first of these warnings appeared whenever the complainant added a new withdrawal address to the whitelisting. This takes the form of a full-screen pop-up. A similar warning appears at the time of each withdrawal, whether or not the withdrawal address is newly whitelisted or it is a withdrawal address which has already been whitelisted and sent on a previous occasion. Both pop-up warnings specifically warned the complainant against scams and to not whitelist or withdraw digital assets to 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 warning displayed during withdrawals, the complainant was further warned that the withdrawals are irreversible. The complainant was also encouraged to learn more about the safety and protection from scams by clicking the link 'Learn More'. This link would have taken him to the regularly updated Crypto.com Help Center page titled '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, specifically agreeing to and acknowledging that the withdrawals were irreversible and the service provider would not be liable for assets sent to the external wallet.

The service provider would also like to highlight the following points. Part of the complaint relates to the allegation that the slow response from the service provider's customer service caused delay in the complainant's ability to recover

his funds. However, the claimant had admitted in the last hearing that all the withdrawals were made by him. As such, he would have had emails from the service provider for each whitelisting and withdrawal with records of the withdrawal details, including the recipient wallet of the funds.

The service provider submits that it is not in possession of any additional information which would have assisted the complainant in recovering his funds.

In spite of the numerous warnings mentioned provided by the service provider, the complainant proceeded to make the withdrawals to the external wallets whilst negligently disregarding the warnings.

Lastly, there was nothing in the service provider's controls, as well as the control of our third-party monitoring tools, to indicate that there was any malicious or scam activity involved in these cases at the material time. The complainant's concerns regarding the disputed transactions were not communicated or brought to the attention of the service provider until after these transactions had already been completed.

Insofar that the transactions have been completed to the full satisfaction of what we were asked to execute on behalf of the complainant himself, the service provider does not bear any responsibility for any loss in regard to these transactions."[10]

The Arbiter had requested submission of copies of the evidence and of warnings given to Complainant at the time of whitelisting the recipient wallets and at the time of transfers.[11]

On being cross-examined, Pema Fung said:

"The complainant is sorry but he did not remember that he introduced any name of someone in the transactions. He simply sent it to the other cryptocurrency email address. And that he didn't remember really that I had found (?) any name in the transactions.

[10] P. 247 - 250
[11] P. 242 - 246

I say that what would have happened in his case is that he would have ticked this wallet. The Complainant is the owner, so he would not have had to fill in any details about it.

The Complainant fully acknowledges that he sent the money himself. It is said that in the document that he has received today, there were two alerts and he made four transfers. And this means that not all transactions were flagged.

The Arbiter interjects to state that he understood that four transfers were sent to two different extended wallets which were non-custodial. So, the Complainant had to actually whitelist two external wallets. So, there are two whitelisting warnings telling the Complainant that he has to be careful that he is whitelisting wallets and he has to be careful. Following that, there were four transfers and for each transfer there is a warning again.

Asked whether this is correct, I say, that this is correct.

Asked why the warnings were more personal or more contextualized because the Complainant believes that more personalized and more contextualized warnings have more impact and one can perceive the risk differently.

I say that these warnings, as the Complainant mentioned, are general warnings because at the time of his transactions, there was nothing in our systems to indicate that there is anything wrong with these transactions. They are just warnings that we send to each and every withdrawal. Now, if we had noticed that the Complainant was sending funds, for example, to a wallet that had been reported or linked to a scam, his transaction would not have been gone through if it was a confirmed scam wallet. This is only a general warning. It has nothing to do with any indications that we were aware of.

The Complainant asks why was it not possible to detect a potential fraud pattern since, in his case, he sent the money three times in the same cryptocurrency wallet address in significant amounts; and asks was it possible for Crypto.com with all the tools that they have not to detect a fraud pattern since the Complainant was a beginner in the crypto domain; wouldn't there be more protection for beginners, for first users in the crypto domain.

As mentioned earlier, nothing in our systems had detected anything that would have suggested fraud or alerted us to any warnings.

Further, the instructions were received from the Complainant's own account which he logged in with his own login credentials, on his own mobile device, and as admitted by himself, were made by him."[12]

The Arbiter requested Foris to submit copies of the declaration they claim Complainant made that he was the beneficial owner of the transferee non-custodial wallets.

This was included in the final submissions.[13]

In a somewhat strange initiative by Complainant, he submitted without being asked, a declaration[14] that he was the owner of a non-custodial wallet ending EB9758 which is different from the 2 wallets addresses relating to where his fraudulent transfers of USDC/USDT were sent.

The Arbiter sees no connection of this declaration to the merits of the case (even though in it the Complainant wrongly states he is making this declaration at the request of the Arbiter).

The Complainant also submitted that he made a police report of the scam and a claim on his Belgian Bank, Fortis, but they could not provide any help with the recovery. Fortis denied responsibility as the transfers were made showing Complainant himself as beneficiary.

Final Submissions

The final submissions of the Complainant[15]consisted of 50 pages rather than the brief summary requested by the Arbiter without new evidence.[16] The said submissions are basically a repetition of what he had already presented in the complaint and in his evidence and added fresh evidence details which cannot be considered at this stage.

In their final submissions, the Service Provider largely repeated their defence of no responsibility for the fraud and submitted the evidence requested by the Arbiter regarding beneficiary ownership of the self-hosted wallets where the

[12] P. 250 - 251
[13] P. 313
[14] P. 254
[15] P. 256 - 305
[16] P. 252

fraudulent transfers were sent. They further elaborated on their defence that such declaration rendered them fully compliant with MICA and Travel Rule regulations by stating:

"***Risk Assessment and Transaction Monitoring under the EU Regulations***

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.

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.

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.

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.

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.

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.

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.

Notwithstanding and without prejudice to the above, the Respondent submits in reference to Travel Rule Regulation, 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 crypt-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 EUR1 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 wallets, 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.*

In this case, the Complainant confirmed that the External Wallets belonged to him by ticking the corresponding box the in the pop-up form.

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 248 of the complaint file wherein it was stated that:

"The complainant would have had to complete the Travel Rule form which asked jo, to indicate whether the external wallet to which funds were being transferred was self-hosted or otherwise, and also 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. 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.

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.

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.

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."[17]

Analysis and Observations

Having heard the parties

Having seen all the documents

Considers

Background about the Scam

It is pretty evident that the Complainant is a victim of a scam.

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 and credibility of the events outlined in the Complaint and the ensuing proceedings; the solemn declaration of the Complainant, testimony and evidence produced.

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 among the first complaints being adjudicated by the Arbiter which tests the additional responsibilities of a service provider licensed under the VFA Act/

[17] P. 308 - 311

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.[18]

The TFR Recast was published in 2023 and, in the case of crypto-asset service providers (CASPs), became applicable from 30 December 2024. (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 introduced **enhanced anti-money laundering (AML) and counter-terrorist financing (CTF) requirements** for **crypto-asset service providers** 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.

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.

[18] The Service Provider's VFA licence was surrendered on 27 January 2025, with the MiCA license issued on the same day.

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"*.[19]

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. 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

[19] As argued by the Service provider p. 309 para. 26

the Service Provider and whether any such failure caused and contributed to the losses suffered, as the Complainant is arguing in this Complaint.[20]

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.[21] 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[22] where it was *inter alia* noted that:

> *"Din il-Qorti tibda billi tqis li l-Arbitru korrettament ikkonstata li s-soċjetà appellata kellha obbligazzjonijiet ta' natura fiduċjarja …"* [23] [24]

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

[20] In his complaint (p.7), the Complainant claims his loss was caused by lack of AML monitoring generally and breach of the expected due diligence under AML Directive 2015/849. As the payments were made in 2025 the Arbiter takes into consideration how the AML regulations were amended effective 30.12.2024 with the introduction of MICA and Travel Rule.

[21] 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.'*

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

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

[24] Unofficial translation, *"This Court considers that the Arbiter correctly established that the appealed entity had fiduciary obligations…"*

best interests of clients.[25] It remained similarly subject to the same principles and requirements under the MiCA regime.[26]

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

[25] 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.'

[26] 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[27] ('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".*[28]

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.[29]

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[30] 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 wallets.

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).

---

[27] https://www.eba.europa.eu/sites/default/files/2024-07/6de6e9b9-0ed9-49cd-985d-c0834b5b4356/Travel%20Rule%20Guidelines.pdf

[28] *Ibid.*

[29] https://fiaumalta.org/app/uploads/2024/12/Dec-2024-Travel-Rule-Guidelines.pdf

[30] Per para. 77 of the Guidelines, being information necessary to determine whether or not a recipient wallet is a self-hosted wallet (external wallet)

In this particular case, the Complainant ticked the box[31] 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 paragraphs 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 paragraph 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;*
>
> *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;"*

[31] *Ibid*.

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;*
>
> *a) the robustness of the assessment each method can deliver;*
>
> *b) 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.

The Service Provider asserts that by simply ticking the box declaring himself of the owner/controller of the transferee wallets, they were in compliance with the Travel Rule regulations:

> ***"In reliance on the Complainant's own declaration, the Respondent satisfied the applicable Travel rule regulations …".***[32]

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.

[32] P. 311 point 31

Reference is also made to the term '**fully satisfied'** in Paragraph 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."*

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[33] 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;

[33] 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)

(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:

a) a post from its website titled *'European Union – Travel Rule Requirements FAQ'*;[34]

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.

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 to be 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 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

[34] https://help.crypto.com/en/articles/10190809-european-union-travel-rule-requirements-faq

(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"*. 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 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."*

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

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 document three authorised methods[35] for the purpose of whitelisting and confirmation of the wallet control and ownership, namely as follows:

(i) the Satoshi Test (on-chain verification)[36]

(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.[37]

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

[35] Seemingly to address the verification methods outlined in EBA Guideline 83, namely 83(c), (d) and (e).
[36] 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

[37] 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/

> *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****."* [38]

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).[39]

As outlined in Article 14(5), *"… 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****"*.[40]

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 30 January 2026 and final submissions.[41]

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.

[38] Emphasis added by the Arbiter
[39] 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".*
[40] Emphasis added by the Arbiter
[41] P. 308, point 24

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.

The Arbiter accordingly does not share the Service Provider's opinion that *"it was under no obligation to raise additional questions"*[42] as it was entitled to rely on the Complainant's self-declaration of ownership.

In its final submissions, the Service Provider additionally referred to Article 16(2) of the TFR Recast[43]. 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 hereby considers whether the fact that the Complainant did not specifically refer to the MICA and Travel Rule obligations in his general complaint (that Foris was responsible for her loss and should be ordered to make full

[42] P. 311 point 32
[43] P. 310 point 29(a)

refund) exempts the Service Provider from any failings in this regard even if they were responsible for contributory causes of the loss.

The Arbiter feels that the obligations resulting from regulation apply in all circumstances and any consumers failure to quote specific chapter and verse in their specific complaint does not exempt Service Providers from liability which would apply if consumers had specifically invoked such references.

The Arbiter notes that in their evidence the Service Providers put up a lengthy defence of their claimed non-liability under MICA and Travel Rule regulations and therefore admitted the need to make their case even if the Complainant had made no specific reference to such obligations.

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 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, the incorrect disclosures the Complainant herself 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; and also given that the Complainant kept interacting and following the instructions of the scammer to the point of executing and authorising transfers to external wallets which effectively were under the control of the scammer.

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),[44] 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…"*,[45] 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"*,[46] and

[44] 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

[45] 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

[46] 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 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.

The Arbiter accordingly decrees that the Service Provider should bear 40% of the loss of €11,163 and compensate the Complainant the amount of €4,465 for its failure to offer Complainant the protection afforded by MiCA and Travel Rule regulations.

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 €4,465 (four thousand, four hundred and sixty-five euro) being 40% of the loss suffered by the Complainant.

With interest at the rate of 2.15% p.a.[47] from the date of this decision till the date of payment.[48]

The Arbiter decrees that there is no case for additional compensation caused by the claimed delay in providing information as such information was already available to Complainant and has not effectively contributed to the loss incurred.[49]

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

This decision is being brought to the attention of MFSA (Malta Financial Services Authority) and FIAU (Financial Intelligence Analysis Unit).

_____

Alfred Mifsud
Arbiter for Financial Services

<u>Information Note related to the Arbiter's decision</u>

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.

[47] Equivalent to the current Main Refinancing Operations (MRO) interest rate set by the European Central Bank.
[48] 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.
[49] P. 207

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.