Before the Arbiter for Financial Services

Case ASF 254/2025

UD

('the Complainant')

vs

Foris DAX MT Limited

(Reg. No. C 88392)

('Foris' or 'Service Provider')

Sitting of 29 May 2026

The Arbiter,

Having seen the Complaint made against Foris DAX MT Limited relating to its alleged failure to warn client that his transfer of digital assets (which digital assets were funded by transfer of Euro currency from his bank account with LCL (Le Credit Lyonnais) in France to his account with Service Provider) to a fraudulent platform, has caused him a financial loss for which he is seeking compensation of €96,000[1].

The Complaint[2]

In his complaint form to the Office of the Arbiter for Financial Services ('OAFS'), the Complainant submitted that he was a victim of a cybercrime perpetrated by fraudulent persons who purported to be representatives of Financial Star Academy to which he was attracted in October 2024 through advertising on social media offering educational services leading to investment opportunities.

[1] Page (p.) 4

[2] P. 1 – 7 with supporting documentation on P. 8 - 20.

He was then contacted by persons who introduced themselves as Jenny Larr and Eric Trousseau who directed him to an investment platform 'Vatradecoin', on which he registered in November 2024.

Foris acknowledged the transactions shown in the Table below.

Sequence number	Date	Amount in EURO	Received by Service Provider	Converted to digital assets and transferred out on
1	13.11.2024	3,241	p. 25	13.11.2024
2	15.11.2024	2,000	p. 25 - 26	15.11.2024
3	19.11.2024	4,000	p. 28 - 29	19.11.2024
4	26.11.2024	6,000	p. 29 - 30	26.11.2024
5	02.12.2024	6,000	p. 30	02.12.2024
6	05.12.2024	1,000	p. 31	05.12.204
7	05.12.2024	9,000	p. 32	05.12.2024
8	18.12.2024	9,500	p. 33	18.12.2024
Sub-total		40,741		
9	03.02.2025	9,850	p. 34	03.02.2025
10	04.02.2025	6,484	p. 35	04.02.2025
11	07.03.2025	26,000	p. 36	07.03.2025
Total		**83,075**		
Transfer by exchange of digital assets		Sold digital assets	Purchased digital asset	Reference
12	15.11.2024	SOL 50	USDT 11394.60	p. 26 exchanged and transferred out on 17.11.2024
13	17.11.2024	UMA 870	UDST 2043.63	p. 27 – 28 exchanged and transferred out on 17.11.2024

This shows 11 transfers in Euro currency of €83,075 (nos. 1 to 11) which were all immediately converted to digital assets and transferred out to external wallets which were not hosted by any Crypto Asset Service Provider (CASP).

It shows two further transfers (no. 12 and 13) which were financed by conversion from other digital assets.

This involved transfers of USDT11394.60 + USDT2043.63 = USDT13,438.23 which added to the Euro transfer of €83,075 roughly explains the claimed loss/compensation of €96,000.

In summary, the Service Provider has acknowledged[3] transfer to external wallets amounting to 0.4919666 BTC and 51760.81 USDT between 13 November 2024 and 07 March 2025[4].

For reasons which will be explained later in this decision, it is important to distinguish between the transfers made in 2024 from those made in 2025 which fall under different regulatory regime which came into force on 30.12.2024. For the time being, it is necessary to establish that the transfers to external wallets made in 2025 under the new regime relate to these payments:

9	03.02.2025	9,850	p. 34	BTC 0.102766
10	04.02.2025	6,484	p. 35	BTC 0.0663535
11	07.03.2025	26,000	p. 36	BTC 0.3117879

Complainant maintains that Service Provider should have detected the irregularity of the transactions on his account and therefore held them responsible for the loss.

He claims that Foris should have protected him from sending his assets to the wallets controlled by the fraudsters and quoted various references to French law on this matter[5].

Complainant denied he was guilty of gross negligence as he had not disclosed any personal data to third parties[6]. He then quotes various transaction monitoring obligations related to banks and finally concludes as follows:

> *'In this case (Complainant) made no error and disclosed no personal data to third parties. Therefore Crypto.com* (brand name of Foris) *must return the funds as no fault can be attributed to (Complainant).[7]'*

[3] P. 36
[4] USDT, SOL, UMA, BTC are all abbreviations of popular digital assets traded on blockchain.
[5] P. 9 - 11
[6] P. 10
[7] *Ibid*.

Service Provider's reply

Having considered in its entirety, the Service Provider's reply[8]

Where the Service Provider provided a summary of the events which preceded the Complainant's formal complaint and explained and submitted the following:

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 29 January 2022.*
- *The Company notes that in the submitted complaints file, the Complainant's representative has outlined his desired remedy as: (i) reimbursement for incurred financial losses*.'[9]

The Service Provider then provided a timeline for the transactions of the Complainant's account with them. These included above listed inward transfers of Euro fiat currency and their conversion to digital assets and transfers out to non-hosted external wallets.

The Service Provider concluded that:

[8] P. 24 - 39 with attachments from p. 40 - 57
[9] P. 24

'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 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 have provided numerous warnings regarding withdrawals to non-custodial wallets.

The first of these warnings appears 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. 40. 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. 41.

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. 42 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 wallets and the fact that they are not hosted or operated by the Company, 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.'[10]

Decree

Following a decree[11] issued by the Arbiter on 19 December 2025 requesting more information, the Complainant submitted that:

- He had a degree education level specialising in electric engineering.
- He was an executive in a construction company since June 2022.
- He was a novice in financial matters and had purchased his first crypto asset in January 2022 on advice from friends.
- He was seeing the funds transferred through Crypto.com on the 'Vatredecoin' investment platform which, at the time, he was not aware it was a fraud.
- On the date of the last transfer on 07 March 2025, he was seeing a balance exceeding €1.5 million representing fictitious profits which were never realised.
- He has not initiated any proceedings against LCL, his Bank in France who executed his transfers, as they were not responsible for the transfers to 'Vatradecoin' platform. He registered a complaint against Foris as they executed the transfers to the said fraudulent platform.

With the complaint, he had attached a copy of the report made to the French National Police[12] where he explained how he was duped into this fraud, how he was seeing the astronomical profits on his account and how he paid €40,000[13] to settle the supposed tax in order to release and withdraw his profits.

Hearings

For the first hearing on 13 February 2026, the Complainant confirmed his submissions on oath.

[10] P. 37 - 39
[11] P. 58 - 59
[12] P. 17 - 18
[13] Being payments 9 - 11 in the above table effected in 2025.

On being cross-examined, he confirmed:

'Asked whether between 2022 and 2025 I continued investing a little bit in crypto assets and gaining some more knowledge in crypto assets from the first time to this time, I say that I only invest in Bitcoin and Solana, but only after the Financial Star Academy contacted me.

Asked whether it is correct to state that the transactions totaling €96,000 were authorised and executed by me, I say, yes.

Asked whether it was the Financial Star Academy who provided me with the wallet address in which to transfer the money, I say, yes.

It is said that in the additional submissions following the Arbiter's decree, I said that I did not initiate any proceedings against my bank, LCL, as the latter was not responsible for the transfers made to the Vatradecoin platform.

Asked for clarification of this and why I do not think that this is necessary, I say that I already had a few cryptos in Crypto.com and I did not see any issue with LCL. And I felt that it was no use making a complaint against them because Crypto.com are known, and I did not see any anomaly between the transfers from LCL to Crypto.com.

Asked whether being a qualified electrical engineer I did not find it reasonable or prudent for me to seek advice prior to entering into this engagement and in something for which I call myself a novice, I say that I believed in the fact that Crypto.com was well known and not fraudulent, and I made research on it, but I could not believe that they would lead me to such a platform. Maybe I was naïve, but I really did not think that the platform was a scam.

I am being referred to page 18 of my complaint (the police report in English) where I said that I was going to file a complaint against X, who may be Eric Rousseau and Jenny Larr and the Financial Star Academy.

Asked whether I have done so, I say that, indeed, I made a complaint against X as his true identity is known; yes, I have made complaints against all the persons that scammed me.

Asked whether I filed proceedings, whether I went to a tribunal or filed anything formally besides the police report, I say that in France when you make

a complaint in front of the prosecutor, you wait for the prosecutor to send the file to the tribunal.

Asked whether it is correct to say that the initial engagement was between me and with the Financial Star Academy who then directed me to invest with Vatradecoin. So, the only link with Crypto.com was the transfer that was made from my bank to Vatradecoin as instructed by Financial Star Academy through an account in my name with Crypto.com.

I say, technically, yes. Financial Star Academy prompted me to transfer to Crypto.com.

Question from the Arbiter to the Complainant:

It is said that there was a sequence of payments which were below €10,000. And, then, the last payment on 7 March was for €26,000.

Asked what the reason was for the sudden move from €10,000 to €26,000, I say that the last lie was that he needed to transfer the money as a percentage of the benefits. So, the $40,000 are composed of the €26,000 of Bitcoin, and he added €14,000 as dividends.

Asked whether I remember, when I was making these transfers to the wallet addresses which were given to me, receiving a warning from Crypto.com for each payment advising me to be sure that I am not dealing with fraudsters and that I know what I am doing, etc., I say, no.

It is said that a lot of transfers were made in 2024, but the last transfers were made in 2025.

It is said that in 2025, a new regulation took effect where I probably had to make a declaration that the wallet I was transferring the funds to belonged to me. Asked whether I remember making that declaration, I say, I followed the process of transferring, but I do not remember anything regarding such declaration.'[14]

[14] P. 88 - 90

The Arbiter requested Service Provider to submit KYC documents filed in 2022 at the establishment of the account relationship with Complainant. This was submitted[15] consisting merely of proof of identification.

At the second hearing on 12 March 2026, Pema Fung for the Service Provider gave evidence by stating:

'The Complainant became a client of the Service Provider on the 29th of January 2022.

The disputed transactions in question relate to 15 withdrawals of cryptocurrency, which was purchased in the complainant's Crypto.com app account. and sent to three external wallet addresses between the 13th of November 2024 and 7th of March 2025.

These wallet addresses are what we refer to as non-custodial addresses, meaning they are not serviced by Crypto.com, and from what is identifiable on the blockchain, they are also not serviced by providers of similar centralised exchanges.

From the evidence at hand and the agreement of the Complainant, these transactions were fully authorised by the complainant and made pursuant to his instructions. Furthermore, the service provider has no affiliation whatsoever with Dogecoin and/or the individuals mentioned, namely, Mr Eric Rousseau and Ms. Jenny Larr.

Insofar as the Travel Rule was applicable to certain transactions, the Complainant was requested to complete the Travel Rule form which asked the user to indicate whether the external wallet to which funds were being transferred to 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 distributed ledger address, and the unique transaction identifier.

[15] P. 96

In this particular case, the Complainant indicated that the wallets were self-hosted, owned and controlled by himself, and this was confirmed via a form submitted by him.

In addition to providing information regarding the destination wallets, warnings were provided as well to the Complainant with each whitelisting and withdrawal.

As these warnings have already been detailed in the Service Provider's reply to the complaint, I will not go into detail here to repeat them. In spite of the numerous warnings provided by the Service Provider at the whitelisting and withdrawal stages, the Complainant proceeded to make the withdrawals to the external wallets, whilst negligently disregarding these warnings.

Lastly, there was nothing in our own controls, as well as the controls of our third-party monitoring tools, to indicate that there is 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 the transactions had already been completed.

Insofar as the transactions have been completed to the full satisfaction of what the Service Provider was asked to execute on behalf of the Complainant, the Service Provider does not bear any responsibility for the loss regarding these transactions.'[16]

No cross-examination of evidence was conducted.

The Arbiter requested Service Provider to submit evidence of the declaration of self-ownership for the last three transfers effected under the MiCA/Travel Rule regime in 2025[17].

Final Submissions

In their final submissions, the parties basically repeated what had already emerged in the complaint, the reply and the hearing proceedings.

[16] P. 91 - 92
[17] P. 99 - 103

The Complainant stressed that Foris had failed to offer him due protection to prevent the fraud and that they had a duty of care and protection to the consumer.[18]

The Service Provider treated the accusation that they failed the duty of care and protection to Complainant with particular reference to the last payments effected under the new MiCA regulation and Travel Rule guidance by stating:

16. *'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.*

17. *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.*

18. *At the material time, the Respondent had no knowledge that there was any fraud history linked to the External Wallets. As has been submitted by the Respondent and unchallenged by any contemporaneous evidence offered by the Complainant, the wallets 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 wallets suspected of illicit behaviour at the time of the Disputed Transactions.*

19. *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.*

[18] P. 108 - 109

20. *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.*

21. *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"):*

22. *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 Complainant does not have a legal basis in terms of the Travel Rule Regulation.*

23. *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.

24. *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, 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 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 bear 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 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.

25. *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.

26. *The Respondent submits that the form was completed and signed using the Complainant's login credentials in which it was expressly stated that the Complainant is the owner of the external wallet in question. By providing this information directly or indirectly through their gross negligence, the Complainant made a clear and affirmative representation as to the ownership and control of the wallet address.*

27. *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 wallet 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.*

28. *The Complainant must therefore bear responsibility for the accuracy and completeness of the information provided. The Respondent was entitled*

to rely on the Complainant's explicit confirmation of ownership and was under no obligation to raise additional questions.

29. *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 where none was warranted.*

Conclusion

30. *In summary, the Respondent would submit that the contractual relationship between the Complainant and the Respondent as set out in the Terms and Conditions clearly provides that the Complainant had the responsibility, among others, to verify all transaction information prior to submitting it to the Respondent and to protect their cryptocurrency wallets/accounts from any unauthorized access. There has been no assumption of risk on the side of the Respondent, and the Complainant has failed to demonstrate the existence of such a duty of care in statutory or case law as applicable to this case.*

31. *In carrying out these transactions, the Respondent has merely carried out the Complainant's transactions as instructed to the External Wallets. On the balance of the foregoing and on the basis of fairness, reasonableness and equity, it is the Respondent's case that the Complainant themself should be responsible for their own alleged losses due to their gross negligence and that costs should be awarded to the Respondent.'*[19]

Having heard the parties

Having seen all the documents

Considers

The fraudulent payments covered by this complaint fall under two distinct regulatory regimes.

[19] P. 114 - 117

The first 8 payments (explained in the Table above nos. 1 - 8) and transfers 12 and 13 were made before the entry into force of MiCA regulation and Travel Rule guidance which kicked into effect on 30 December 2024. The last three payments nos. 9 - 11 for €42,334, were made under the new regulatory regime which obliged enhanced procedures on the Service Provider.

The Arbiter has adjudicated several cases where he dismissed complaints with intrinsically similar characteristics as related to the payments and transfers executed before the MiCA and Travel Rule kicked into effect.

By way of example, see ASF 119/2025[20], ASF 045/2025[21], ASF 054/2025[22], which decisions were issued in 2026 related to cases of complainants assisted by the same legal representative as the Complainant of this case.

All these decisions are now *res judicata* as they have not been appealed.

The Arbiter is obliged by Article 19(3)(d) of CAP. 555 of the Laws of Malta to deal with a complaint in a procedurally fair, informal, economical and expeditious manner. Consequently, to avoid repetition, the Arbiter makes reference to his decisions above referred to, and in a consistent manner uses the same explanations to dismiss any claim for compensation related to the payments and transfers of digital assets to external wallets which were affected before 30 December 2024.

The transfers made under MiCA and Travel Rule regime

The Arbiter will proceed to analyse the claim for compensation related to these payments and transfers:

[20] https://financialarbiter.org.mt/sites/default/files/oafs/decisions/2932/ASF%20119-2025%20-%20TY%20vs%20Foris%20DAX%20MT%20Limited.pdf

[21] https://financialarbiter.org.mt/sites/default/files/oafs/decisions/2575/ASF%20045-2025%20-%20DS%20vs%20Foris%20DAX%20MT%20Limited.pdf

[22] https://financialarbiter.org.mt/sites/default/files/oafs/decisions/2638/ASF%20054-2025%20-%20ZO%20vs%20Foris%20DAX%20MT%20Limited.pdf

9	03.02.2025	9,850	p. 34	BTC 0.102766 ref p. 99 - 100
10	04.02.2025	6,484	p. 35	BTC 0.0663535 ref. p. 101
11	07.03.2025	26,000	p. 36	BTC 0.2811972[23] ref p. 102 - 103

The payments were converted in crypto-asset known as BTC[24] transferred to a self-hosted wallet ending ….UEaQL which Complainant declared himself as the beneficial owner thereof.

The price of BTC on transfer dates was as follows:

03 - 04.02.2025 USD 96,000 x 0.1691195 units BTC = USD 16,235 = €15,762

07.03.2025 USD 82,000 x 0.2811972 units BTC = USD 23058 = €21,154

Total value €36,916 (using official BTC price and ECB rate of exchange for Euro/USD).

Consequently, the Arbiter is considering the total loss suffered under MiCA/Travel Rule regime as €36,916.

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/ 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.[25]

The TFR recast introduced **enhanced anti-money laundering (AML) and counter-terrorist financing (CTF) requirements** for **crypto-asset service**

[23] Although conversion of €26,000 produced 0.3117879 BTC only 0.2811972 BTC were transferred out.
[24] Bitcoin
[25] The Service Provider's VFA licence was surrendered on 27 January 2025, with the MiCA licence issued on the same day and thus before the disputed transactions.

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.

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'.[26]

[26] As argued by the Service Provider p.114 para. 20

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 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.[27]

[27] 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.'*

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[28] 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 …'.*[29]

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 best interests of clients.[30] It remained similarly subject to the same principles and requirements under the MiCA regime.[31]

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.

---

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

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

[30] 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.'

[31] 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.

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 (EBA/GL/2024/11) issued by the European Banking Authority ('EBA') in July 2024[32] ('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'.* [33]

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.[34]

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[35] 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.

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

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'.***[36]

In this particular case, the Complainant ticked the box[37] 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 whitelisted 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:

[36] P. 99 - 103 – in evidence related to similar cases Foris had explained this document signifies that Complainant ticked the box confirming self-hosted wallet was under his ownership.
[37] *Ibid*.

'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;'

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.

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.'*

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[38] 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 reply, the Service Provider only limited itself to providing just the following:

a) a post from its website titled *'European Union – Travel Rule Requirements FAQ'*;[39]

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 official reply[40].

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 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

[38] 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)
[39] https://help.crypto.com/en/articles/10190809-european-union-travel-rule-requirements-faq
[40] P. 54 - 57

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*'.

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.

From evidence collected in similar cases, the Arbiter learned 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 Service Provider argues that in obtaining Complainant's declaration through a tick box procedure that he is the owner of the self-hoisted external wallet, they have honoured their obligations under the new MiCA and Travel Rule regulatory regime.

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[41] for the purpose of whitelisting and confirmation of the wallet control and ownership, namely, as follows:

(i) the Satoshi Test (on-chain verification)[42]

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

[41] Seemingly to address the verification methods outlined in EBA Guideline 83, namely 83(c), (d) and (e).
[42] 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

(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.[43]

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.'***[44]

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).[45]

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'.***[46]

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

[43] 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/

[44] Emphasis added by the Arbiter

[45] 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'*

[46] Emphasis added by the Arbiter

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.

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.

The Arbiter accordingly does not share the Service Provider's opinion that *'Respondent acted reasonably, lawfully and in full compliance with its regulatory obligations by using the information exactly as it was provided by the Complainant … and was under no obligation to raise additional questions.'*[47]

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

[47] P. 117 points 28, 29.

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 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, *'Vatradecoin',* the incorrect disclosures the Complainant himself made that he was the owner/controller of the external wallet; and also given that the

Complainant kept interacting and following the instructions of the scammer notwithstanding that he was already suspecting fraud.

Also, by deciding not to open any proceedings against his French Bank LCL, Complainant is admitting that he was grossly negligent in making these transfers exempting his bank from transaction monitoring obligations under the Directive PSD 2[48].

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),[49] 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 …'*,[50] and

[48] Preamble 71 of PSD 2 (**DIRECTIVE (EU) 2015/2366)** states**:**

*'In the case of an unauthorised payment transaction, the payment service provider should immediately refund the amount of that transaction to the payer. However, where there is a high suspicion of an unauthorised transaction resulting from fraudulent behaviour by the payment service user and where that suspicion is based on objective grounds which are communicated to the relevant national authority, the payment service provider should be able to conduct, within a reasonable time, an investigation before refunding the payer. In order to protect the payer from any disadvantages, the credit value date of the refund should not be later than the date when the amount has been debited. In order to provide an incentive for the payment service user to notify, without undue delay, the payment service provider of any theft or loss of a payment instrument and thus to reduce the risk of unauthorised payment transactions, the user should be liable only for a very limited amount**, ***unless the payment service user has acted fraudulently or with gross negligence****. In that context, an amount of EUR 50 seems to be adequate in order to ensure a harmonised and high-level user protection within the Union. There should be no liability where the payer is not in a position to become aware of the loss, theft or misappropriation of the payment instrument. Moreover, once users have notified a payment service provider that their payment instrument may have been compromised, payment service users should not be required to cover any further losses stemming from unauthorised use of that instrument. This Directive should be without prejudice to payment service providers' responsibility for technical security of their own products*.' (emphasis added by Arbiter)

[49] 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

[50] Page 4 of the FATF, Best Practices, Travel Rule Supervision, June 2025:

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*'[51], and

- 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.

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 40% of the loss suffered by the Complainant through the above-listed transfers effected in

https://www.fatf-gafi.org/content/dam/fatf-gafi/recommendations/Best-Practices-Travel-Rule-Supervision.pdf

[51] Page 3 of EBA's Final Report (EBA/GL/2024/11]

2025 resulting in a loss of €36,916 as above explained. Consequently, the Arbiter orders a compensation of €14,766 (fourteen thousand, seven hundred and sixty-six euro).

With interest at the rate of 2.15% p.a.[52] from the date of this decision till the date of payment.[53]

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) it being among the first of its kind since the Travel Rule regulation came into effect and, also, to consider any regulatory issues related to the scant provision of KYC documentation.

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

[52] Equivalent to the current Main Refinancing Operations (MRO) interest rate set by the European Central Bank.
[53] 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.

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.