Before the Arbiter for Financial Services

Case ASF 235/2025

TC

('the Complainant')

vs

Foris DAX MT Limited

(Reg. No. C 88392)

('Foris', 'Foris DAX' or 'Service Provider')

Sitting of 17 July 2026

The Arbiter,

Having seen the Complaint made against Foris DAX MT Limited relating to its alleged failure to warn the client that his transfer of digital assets (which digital assets were funded by transfers of Euro currency from his bank account with Crédit Agricole 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 €295,138[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 crypto investments via a trading platform Trade Pro, which promoted crypto-assets trading as an easy way to get rich and which was being followed by prominent French personalities.

[1] Page (P). 4
[2] P. 1 - 7 with supporting documentation on P. 8 - 62.

Foris acknowledged in their reply to OAFS the transactions shown in the Table A below.

Table A

Sequence number	Date	Amount in EURO	Received by Service Provider	Converted to digital assets and transferred out immediately
1-2	20.05.2024	3,010	P. 67 - 68	ETH 0.86044
3	22.05.2024	2,600	P. 68 - 69	ETH 0.72837
4	25.06.2024	10,000	P. 69 - 70	ETH 3.08979
5	04.07.2024	5,000	P. 70 - 71	ETH 1.66243
6	06.08.2024	5,000	P. 71 - 72	BTC 0.0957423
7	27.09.2024	2,000	P. 74	ETH 0.79863
8	01.10.2024	8,600	P. 75 - 76	ETH 1.71154 + 1.95894
9	03.10.2024	10,000	P. 76 - 78	ETH 2.2702 + 2.26965
10	08.10.2024	18,000	P. 78 - 80	ETH 3.51902 + 2.19565 +2.19733
11	17.10.2024	16,600	P. 80 - 81	ETH 6.6677
12	25.10.2024	12,000	P. 81 - 82	ETH 4.91667
13	05.11.2024	21,800	P. 82 - 84	ETH 4.30001 + 5.05155
14	15.11.2024	21,800	P. 84 - 85	ETH 7.14317
15	21.11.2024	14,388	P. 85 - 86	ETH 2.43547 +2.23658
16	11.12.2024	28,500	P. 87 - 88	ETH 7.774475
17	23.12.2024	20,800	P.88 - 89	ETH 6.300694
18	24.12.2024	25,000	P. 89 - 90	ETH 7.312035
19	26.12.2024	15,000	P. 90 - 91	ETH 4.496259
SUB-TOTAL 2024		**240,098**		
20	14.01.2025	15,000	P. 91 – 92	ETH 4.69396849
21	17.01.2025	10,000	P. 92 - 93	ETH 2.875944
22	27. 01.2025	30,000	P. 93	ETH 9.921079
23	29.01.2025	40	P. 94 – 95	ETH 0.00811
SUB-TOTAL 2025		**55,040**		ETH 17.49910
TOTAL		**295,138**		

In addition to the above payments/transfers, Service Provider reported a transfer inward for €14,852.4 on 08.08.2024[3] which was immediately converted to ETH and transferred out in several instalments to external wallets between 09.08.2024 and 13.08.2024. On querying this payment, which is not part of the complaint, Complainant explained that these were transactions effected by the fraudster from which he suffered no loss[4].

As this claim revolves around digital assets transferred out to external wallets, one can summarise the loss claimed as follows:

a) Transfers 1-19 in Table A above were all effected before 30.12.2024. For reasons which will be explained later, these are not considered by the Arbiter as qualifying for any compensation.

b) Transfers 20-23 in Table A above were all effected in 2025 and involve transfers of ETH 17.49910 funded by transfers of €55,040.

   As these transfers took effect in 2025, they may qualify for compensation.

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 a different regulatory regime which came into force on 30.12.2024.

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

He claims that Foris should have protected him from sending his assets to the wallets controlled by the fraudsters[5] and quoted various references to French law on this matter.[6]

Complainant denied he was guilty of gross negligence as he had not disclosed any personal data to third parties[7]. He then quotes various transaction monitoring obligations related to banks and finally concludes as follows:

---

[3] P. 72
[4] P. 147
[5] P. 95 - Service Provider lists 13 different wallet addresses to which the digital assets (mainly ETH) were transferred.
[6] P. 10 - 12
[7] P. 12

"In this case [Complainant] did not make any mistakes. Furthermore, he did not disclose any personal data to third parties.

Consequently, … Crypto.com [brand name of Foris] must return the funds to [Complainant] as the latter did not commit any wrongdoing." [8]

Service Provider's reply

Having considered in its entirety the Service Provider's reply:[9]

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*[10]

- That Foris DAX 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.

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

- That the Complainant became a customer of Foris DAX through the Crypto.com App and was approved to use the Wallet on 20 May 2024.

- That it notes that in the submitted complaints file, the Complainant's representative has outlined his desired remedy as reimbursement for incurred financial losses.

The Service Provider then provided a timeline for the transactions of the Complainant's account with them. These included the above-listed inward

---

[8] *Ibid*
[9] P. 66 - 98 with attachments from p. 99 - 142
[10] P. 66

transfers of Euro fiat currency and their conversion to digital assets and transfers out to non-hosted external wallets.

The Service Provider concluded that:[11]

- Based on its investigation, it was unable to honour the Complainant's refund request based on the fact that the reported transfers were made by the Complainant himself.

- Whilst Foris sympathises with the Complainant and recognises that he may have been misled or induced into transferring funds to an alleged fraudster, it is important to note that these transfers were made solely at the Complainant's request. It also emphasised that the addresses the funds were transferred to, do not belong to the Company and as such, any due diligence of the ownership of these addresses falls under the responsibilities of the provider of said wallets.

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

- That the Complainant is solely responsible for the security and authenticity of all instructions submitted through his Wallet as outlined in the Foris DAX MT Limited Terms & Conditions.

- That the relevant section of the Terms & Conditions stipulate:

    "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

[11] P. 96 - 98

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 Service Provider pointed out that 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.

2. *Service Provider's Warnings*

That 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 appears whenever a user adds a new withdrawal address to the Crypto.com App. For the reference of the OAFS, the warning appears as below, in Fig. 110 of its reply.[12] 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

[12] P. 139

already been whitelisted on a previous occasion. An example of this warning can be found below, exhibited as Fig. 111 to its reply.[13]

That, as can be seen from the examples provided, 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 was further warned that the withdrawal was irreversible.

Foris further submitted that 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 was labelled as Fig. 112 to its reply).[14]

It also noted that upon the Complainant confirming that he had read the scam warning by clicking on the *"Confirm and Withdraw"* button on the pop-up warning, the Complainant confirmed he 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.

Foris submitted that in spite of the numerous warnings mentioned above, the Complainant proceeded to make the withdrawals to the External Wallets. It noted that the Complainant either negligently disregarded the warnings or was otherwise unaffected by them.

3. *Summary provided by Foris in its reply*

That, 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

[13] P. 140
[14] P. 141

and the fact that they are not hosted or operated by Foris, the Service Provider can neither confirm nor deny this.

Whilst Foris fully empathises with the Complainant in this regard, it submitted that 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.

That as outlined above in the Foris DAX MT Limited Terms of Use, the Complainant is solely responsible for the security and authenticity of all instructions submitted through the Crypto.com App, and as such, Foris cannot accept liability for the veracity of any third-party or for the instructions received from the Complainant themselves.

Decree

Following a decree[15] issued by the Arbiter on 19 December 2025 requesting more information, the Complainant submitted that:

- He had an education level of an Associate's degree.
- He was employed as a manager of a service company.
- He had no experience in investments or crypto-assets.
- He was seeing the funds transferred through Crypto.com on the *'Trade Pro'* investment platform, which at the time he was not aware was a fraud.
- He no longer had access to the platform, so he could not say how much profit he was seeing on the platform at the time of his last payment in January 2025.[16]
- He filed a complaint with his French Bank seeking reimbursement of his loss.[17]

[15] P. 143 - 144
[16] Even during the hearings, Complainant avoided giving any indication of such profit (fictitious) he was seeing on the platform. He provided a screenshot (p. 163) showing value of USDT395.860 which seems dated 29 January (2025?).
[17] P. 150 - 155

Hearings

For the first hearing on 25 February 2026, the Complainant confirmed his submissions on oath and confirmed that all transfers from his wallet were authorised by him.

On being cross-examined, he stated:[18]

1. Crypto.com was not in any way involved in his dealings with representatives of Trade Pro.
2. Credit Agricole rejected his complaint and they are in the process of seeking mediation with possible decision in April/May 2026.
3. In June 2025, he filed a report of the scam to the French Prosecution Office (translated copy requested but not submitted).
4. He did not remember receiving any warnings from Foris when authorising the transfers. He stated that when he started having doubts he tried to reach out unsuccessfully to crypto.com.
5. He was directed by the scammers to route his payments via Crypto.com

He also stated:[19]

> *'I say that this was while the scam was going on and when I began to have doubts regarding the operations and transfers.*
>
> *Asked who were these stockbrokers and where did they say they were calling from, I say that, initially, the first ones claimed to be affiliated with the Trade Pro platform. However, subsequently, there were so many interlocutors that I did not know who was from where. They kept contacting me regarding problems with the files without disclosing where they come from or anything on that nature.*
>
> *It is said that a number of transactions took place between May 2024 and January 2025.*

[18] P. 165 - 167
[19] P. 165 - 166

Asked whether I tried and actually withdrew money which belonged to me; whether throughout the entire transaction period, excluding the initial small withdrawal, I actually made any withdrawals from these alleged profits, I say that I wanted to withdraw money when I saw the profits, but each time I requested it, they asked for more money. I made a few withdrawals of very small amounts, such as €10 maximum, but no more. Therefore, with the exception of those minimum amounts, the answer is no.

Asked whether I sought any advice from anyone at a bank or from someone who understands financial services or crypto before making all these transactions, I say, no. No one advised me before I made the investment. The only time I received advice was when I began to feel something was wrong. The expert I consulted confirmed that something suspicious was going on.

Asked when this was, I say that I requested classes on trading at the end of 2024. I attended these for two or three months for approximately an hour and a half each week. It was through these classes, and by asking my teacher questions that I started to understand what was happening.

I say I started in November 2024. I had a class every week or two. It lasted from November 2024 until February 2025. At the end of the course, whilst speaking with my teacher, the teacher advised me to stop because it was fraudulent.'

At the second hearing held on 18 March 2026, an official of the Service Provider gave evidence by stating:[20]

'The Complainant became a client of the Service Provider on the 20th of May 2024. And the disputed transactions in question relate to 54 withdrawals of cryptocurrency, which was purchased in the Complainant's Crypto.com app account and sent to 13 different external wallet addresses between 21st of May 2024 and 29th of January 2025.

These wallet addresses are what we call non-custodial addresses which means that they are not hosted by the Service Provider or identified from the

[20] P. 168 - 171

data on the blockchain as provided by service providers of similar crypto exchanges.

From the evidence at hand and the agreement of the Complainant himself, these transactions were fully authorised by him and made pursuant to his instructions.

For the avoidance of any doubt, the Service Provider does not have any affiliation whatsoever with Trade Pro and/or the individual mentioned, namely, Ms Marion Maréchal-Le Pen.

With regard to the four withdrawals which were performed in January 2025, these transactions were made to a connected Crypto.com on-chain wallet belonging to the Complainant.

The on-chain is a completely separate self-custodial wallet. It is a product serviced by Growth Labs, a company incorporated in the Cayman Islands.

Customers of these on-chain wallets fully control their private keys and their cryptocurrency inside these wallets.

On-chain wallet holders can choose to connect their on-chain wallets to their Crypto.com app account to enable them to transfer funds in between the two accounts, the two wallets.

In order to connect an on-chain wallet to the Complainant's app account, Crypto.com app account, the Complainant would have needed to access his onchain wallet and click the Connect Crypto.com account button from within his on-chain wallet.

He would then have to enter his email account to which his Crypto.com app account was registered to in order for us to send a connection request email to his email address.

To connect an on-chain wallet to a Crypto.com app account, the Complainant would have also had to tick a box stating, 'I confirm that I am the ultimate beneficial owner of both the Crypto.com app and OnChain. The funds transferred from the Crypto.com app to OnChain are my own funds. I am acting for myself and not for any third parties.'

An email would be sent to the registered Crypto.com app account email. From there, the Complainant would then have to click the Connect tab from the email received.

Therefore, in order to connect an on-chain wallet to a Crypto.com app account and withdraw funds from the on-chain wallet, the person would have to have access to OnChainWallet and, also, the registered email account of the Crypto.com app account and, of course, access to the Crypto.com app account to make any withdrawals.

However, as the on-chain wallet is a self-custodial wallet, the Service Provider does not have any control over the on-chain wallet as mentioned above, but merely the on-chain wallet is connected to allow the user to move assets between the two wallets.

Furthermore, during the course of the Complainant's disputed transactions, the Service Provider had provided numerous warnings in place at the material time regarding withdrawals to external wallets.

The first of these warnings would appear whenever the Complainant added a new withdrawal address, known as whitelisting, and take the form of a full screen pop-up.

Similar warnings appeared each time a withdrawal was made whether or not this was to a newly whitelisted withdrawal newly or to a withdrawal which has already been whitelisted 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 warnings displayed during the 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 named 'Avoiding Digital Currency Scams.'*

Upon the Complainant confirming that they had read the scam warnings by clicking on the 'Confirm and Withdraw' button of the pop-up warning, the Complainant confirmed they 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 that the Service Provider would not be liable for assets sent to the external wallets.

In spite of these numerous warnings, the Complainant proceeded to make the withdrawals to the external wallets whilst negligently disregarding the warnings.

It is noted that the screenshots of these warnings were not included in the Service Provider's reply. Should the Arbiter require this evidence, we will be happy to include it if necessary.

Lastly, there was nothing in our own controls as well as the controls 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 been completed.

Therefore, insofar as the transactions have been completed to the full satisfaction of what we were asked to execute on behalf of the Complainant, the Service Provider does not bear any responsibility for any loss in regard to these disputed transactions.

Lastly, with regard to the on-chain wallet connection procedure, should the Arbiter require screenshots of the process to give him a clearer picture of how this is done, we will be happy to provide screenshots as well.

… The Arbiter asks [the Service Provider's official] since she seems to have made emphasis that the question of the on-chain payments related to the payments of 2025 whether there is a clear cut that all the other payments of

2024 were made to a normal external wallet and only the payments of 2025 were made on with the on-chain system.

[The official] replies: … I believe that a number of withdrawals beginning from the 24th or the 23rd of December 2024 were made to the same on-chain wallet. It is correct to say that it starts on the 23rd of December 2024 and keeps going till the end.'

No cross-examination of evidence was conducted.

The Arbiter requested the Service Provider to submit evidence of:

1. the declaration of self-ownership for the last transfers effected under the MiCA/Travel Rule regime in 2025[21].
2. Copies of KYC documents taken when on-boarding the Complainant[22].
3. Copies of screenshots related to the procedure to link the on-chain wallet to the Crypto.com wallet[23].

Final Submissions

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

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.[24]

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:[25]

'18. 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.

[21] P. 177 - 187
[22] P. 187; 207 - 208
[23] P. 177 - 186
[24] P. 174 - 175
[25] P. 191 - 194

19. *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.*

20. *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.*

21. *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.*

22. *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.*

23. *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").*

24. *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 Complaint does not have a legal basis in terms of the Travel Rule Regulation.

25. *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.*

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

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

(a) Article 14(5) of the Travel Rule Regulation provides as follows: "In the case of a transfer of crypto-assets made to a self-hosted address, the crypto asset provider of the originator shall obtain and hold the information referred to in paragraphs 1 and 2 and shall ensure that the transfer of the crypto-assets can be individually identified.

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

Similarly, Article 16(2) of the Travel Rule Regulation provides that: "In the case of a transfer of crypto-assets made from a self-hosted address, the crypto-asset service provider of the beneficiary shall obtain and hold the information referred to in Article 14(1) and (2) and shall ensure that the transfer of crypto-assets can be individually identified.

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

With regards the above legal provisions, the Respondent obtained written confirmation from the Complainant that the transfer and transaction pertaining to the Disputed Transaction was a transfer made to a wallet which the Complainant declared to be 'self-hosted' in compliance with paragraph 78 of the Travel Rule Regulations which adds that "if such information cannot be retrieved via technical means, the originator's CASP and the beneficiary's CASP should obtain that *information [i.e. the terms of whether the counterparty wallet to the CASP is self-hosted or not] directly from its customer." The Respondent submits that it should not be held liable and responsible for any misstatements made by the Complainant. The Complainant was required to provide true and accurate information, however, has provided inaccurate information and is now claiming that Respondent should be the consequences of transfers which were instructed and authorised by the Complainant.*

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

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

27. *Through connecting of the Crypto.com App account to the Crypto.com Onchain wallet, 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.

28. The Respondent submits that the forms were completed and signed through the control and access to the Crypto.com Onchain wallet and using the Complainant's Crypto.com App account login credentials, in which it was expressly stated that the Complainant is the owner of the Crypto.com Onchain 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 Crypto.com Onchain wallet.

29. 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.

30. The Respondent was entitled to rely on the Complainant's explicit confirmation of ownership <u>through both the sending account and receiving end (directly from the Onchain wallet)</u> and was under no obligation to raise additional questions.

31. 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.'

Having heard the parties

Having seen all the documents

Considers

The fraudulent transfers covered by this Complaint fall under two distinct regulatory regimes. The first 19 transfers (explained in Table A above nos. 1-19) were made before the entry into force of MiCA regulation and Travel Rule guidance which kicked into effect on 30 December 2024. The remaining payments no. 20 - 23 for a value equivalent to €55,040 as explained above, 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[26], ASF 045/2025[27], ASF 054/2025[28], 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 effected before 30 December 2024.

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

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

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

The transfers made under the MiCA and Travel Rule regime

These consist of the following transfers:

Table B

Sequence number	Date	Amount in EURO	Received by Service Provider	Converted to digital assets and transferred out immediately
20	14.01.2025	15,000	p. 91 – 92	ETH 4.69396849
21	17.01.2025	10,000	P. 92 - 93	ETH 2.875944
22	27. 01.2025	30,000	P. 93	ETH 9.921079
23	29.01.2025	40	P. 94 – 95	ETH 0.00811
TOTAL - 2025		**€55,040**		**ETH 17.49910**

Consequently, the Arbiter is considering the total loss suffered under the MiCA/Travel Rule regime as €55,040.

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.[29]

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

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

[29] The Service Provider's VFA licence was surrendered on 27 January 2025, with the MiCA license issued on the same day and thus before the disputed transactions.

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'.[30]

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

[30] As argued by the Service Provider p. 191 para. 22.

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.[31] 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[32] where it was *inter alia* noted that:

> *'Din il-Qorti tibda billi tqis li l-Arbitru korrettament kkonstata li s-soċjetà appellata kellha obbligazzjonijiet ta' natura fiduċjarja …'.*[33]

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

---

[31] 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.'*
[32] The exchange of fiat into crypto and the transfer of crypto-assets to other wallets.
[33] Para. 12 page 36 of the Court of Appeal (Inferior Jurisdiction) No. 35/2025 LM.

best interests of clients.[34] It remained similarly subject to the same principles and requirements under the MiCA regime.[35]

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

[34] 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.'

[35] 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[36] ('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'.* [37]

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.[38]

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 cannot be retrieved via technical means, the originator's CASP and the beneficiary's CASP should obtain that information directly from its customer …'.*[39]

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.

In other similar cases already decided against the same Service Provider 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).

[36] https://www.eba.europa.eu/sites/default/files/2024-07/6de6e9b9-0ed9-49cd-985d-c0834b5b4356/Travel%20Rule%20Guidelines.pdf
[37] *Ibid.*
[38] https://fiaumalta.org/app/uploads/2024/12/Dec-2024-Travel-Rule-Guidelines.pdf
[39] P. 193

There was 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.*

In this particular case, rather than merely ticking the box declaring himself to be the beneficiary of the unhosted wallet, there was a whole procedure thoroughly explained by the Service Provider[40], of the process linking a Crypto.com Onchain to a Crypto.com App.

The Arbiter takes into consideration paras. 83 - 86 of the EBA 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 any Complainant's self-declaration of ownership[41] and make its own and further verifications.

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

> *'a) unattended verifications as specified in the Guidelines on the use of Remote Customer Onboarding Solutions under Article 13(1) of Directive (EU) 2015/8499 displaying the address;*
>
> *b) attended verification as specified in the Guidelines on the use of Remote Customer Onboarding Solutions under Article 13(1) of Directive (EU) 2015/849;*
>
> *c) sending a predefined amount (preferably the smallest denomination of a given crypto-asset), set by the CASP, from and to the self-hosted address to the CASP's account;*

[40] P. 177 - 186

[41] During the hearing of 18 March 2026, an official of Foris testified *inter alia* that: *'To connect an on-chain wallet to a Crypto.com app account, the Complainant would have also had to tick a box stating, 'I confirm that I am the ultimate beneficial owner of both the Crypto.com app and OnChain. The funds transferred from the Crypto.com app to OnChain are my on funds. I am acting for myself and not for any third parties'* – P. 169

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.'

The Arbiter is of the firm opinion that the Service Provider had obligations under the Travel Rule to make verifications 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.

The Arbiter therefore has to consider whether the procedure linking the Onchain wallet to the App met the 'fully satisfied' provisions of the Travel Rule guidance above indicated.

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.'***[42]

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).[43]

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'.***[44]

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-*

[42] Emphasis added by the Arbiter
[43] 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'*
[44] Emphasis added by the Arbiter

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.

Does the On-Chain linking procedure satisfy the conditions set in the Travel Rule Guidelines?

As outlined above, in this particular case, rather than merely ticking the box declaring himself to be the beneficiary of the non-hosted wallet, there was a whole procedure, thoroughly explained by the Service Provider[45], of the process linking an Onchain wallet to a Crypto.com App.

1. Fig. 2, presented by the Service Provider in its submissions of 27 March 2026,[46] shows the Complainant willingly linking the Onchain to the App declaring both to be under his ownership.
2. Fig. 3 in the said submissions,[47] he gave his registered email account with Crypto.com for the purpose of confirming the link.
3. The subsequent Fig. 4,[48] shows he wilfully authorised the connection which was confirmed by his passcode as in Fig 5.[49] and 2FA code as in Fig. 6.[50]

[45] P. 177 - 186
[46] P. 179
[47] P. 180
[48] P. 181
[49] P. 182
[50] P. 183

4. As outlined in Fig. 7,[51] he was asked to authorise the connection of which he eventually received a confirmation as in Fig. 8.[52]

5. This connection was eventually confirmed by a specific email as in Fig. 9.[53]

In the evidence that the Service Provider's official gave in the proceedings it was stated under oath that payments made in 2025 (and some of the last payments made in 2024) were made to the external non-hosted wallet which was linked Onchain to the App by the above defined procedure.[54]

By a detailed decree of 29 May 2026, the Arbiter requested further and various clarifications from both parties and gave the parties the opportunity to make submissions on this crucial point.[55]

The Complainant subsequently submitted that the linking process of the Onchain wallet to the Mobile App was dictated to him by the fraudster and he was not understanding what the scope of the procedure was other than that it was necessary *"to allow the transfer of funds to his bank account"*[56]*.*

The Service Provider made a strong assertion that the linking procedure between the Onchain wallet and the app was appropriate to satisfy their obligations under the Travel Rule as they rendered them fully satisfied that the transferee wallet was owned and controlled by the Complainant in terms of his tick box declaration.

Of particular reference are the following assertions:

> *'As admitted by the Complainant in the 'Additional Information' dated 11 June 2026 …, it was the Complainant himself who completed the connection of the Crypto.com App account to the Crypto.com Onchain wallet. As detailed above, in order to do so, the Complainant must have had access to and control of the Crypto.com Onchain wallet as this had to be installed and*

[51] P. 184
[52] P. 185
[53] P. 186
[54] P. 171
[55] p. 195 - 198
[56] P. 200

held in his mobile device in order for the connection process to be successfully completed.' [57]

…

The Service Provider respectfully submits that this verification method is "reliable and secure" within the meaning of paragraph 83(f) of the EBA Travel Rule Guidelines because it can only be successfully completed by a natural person who simultaneously (i) holds the private keys to the OnChain wallet on the device, (ii) has the registered email address of the App account, (iii) has the App login credentials and 2FA/passkey, and (iv) has the OnChain app installed on the same physical device.' [58]

In the circumstances, and on the basis of the submissions made and evidence provided and emerging in this case, the Arbiter is of the opinion that the linking procedure of the Crypto.com App to the Onchain wallet satisfies the Service Provider's obligations under the MiCA Regulations and Travel Rule Guidance requesting it to be fully satisfied that the external wallet linked to the App was under the control of the Complainant[59].

Specifically, it satisfies Article 83 (e) of the Travel Rule Guidelines which state:

'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.'

…

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'.

Whilst sympathising with the Complainant for the terrible ordeal suffered, the Arbiter highlights the need for consumers to seek proper advice and guidance from qualified and verified professionals before it is too late, to exercise great care and attention when making declarations relating to the ownership of

[57] P. 204
[58] P. 205
[59] P. 202 - 206

external wallets and to carefully verify the identity and legitimacy of the recipient before transferring their crypto-assets to external wallets.

Other Observations

The Arbiter notes that as part of its Customer Due Diligence, the Service Provider was aware that the Complainant's *'Expected Annual Transaction'* in respect of his account was of EUR 60,000 (which amount is noted to be below his indicated *'Annual Income'* of over EUR 100,000).[60, 61]

Within just seven months, from May to December 2024, the Complainant had, however, already carried out transactions in total of EUR 240,098, that is, four times his indicated expected annual transactions (and over twice his annual income). Additionally, in just one month, during January 2025, he undertook further transactions of EUR 55,040, nearly equal to the annual expected transaction amount. Hence, the actual total transactions undertaken over an eight-month period correspond to five times the expected annual transactions indicated during the onboarding stage and around threefold his annual income.

Whilst the Complainant had a high six-figure annual income, it has, oddly, not emerged that the above discrepancy triggered any interventions by the Service Provider to, *inter alia*, clarify the operation of the account.

Notwithstanding such apparent lack of intervention which would have reasonably been expected in ordinary circumstances, the Arbiter still finds no sufficient basis on which he can award compensation, given that this matter, on its own, cannot be tangibly attributed as the causal factor of the sustained losses in the case in question.

The transfers were evidently sourced from his own account with his home French Bank which had direct obligations under the payments regulation PSD2 to monitor the regularity of these payments. This is also when taking into account the specific circumstances involving the satisfaction of the Travel Rule

[60] P. 208

[61] This information was not immediately provided by the Service Provider despite that it was requested, during the hearing of 18 March 2026, to present copies of the KYC undertaken at onboarding stage (P. 172). The additional information was only provided further to another specific request about the KYC procedures in the Arbiter's decree of 29 May 2026 (P. 197-198).

requirement as considered above and the OnChain wallet, which indicated a certain level of engagement in dealing with digital assets on the part of the Complainant.

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 particular circumstances of this case, the Arbiter finds no sufficient basis to conclude that the Service Provider did not comply with its fiduciary and duty of care obligations, taking into account the applicable regulatory requirements.

The Arbiter is accordingly not upholding the request for compensation for the loss suffered.

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

Alfred Mifsud
Arbiter for Financial Services

Information Note related to the Arbiter's decision

Right of Appeal

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

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

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