Before the Arbiter for Financial Services

Case ASF 073/2025

IT

('the Complainant')

vs

Foris DAX MT Limited

(Reg. No. C 88392)

('Foris', 'the Company' or

'Service Provider')

Sitting of 24 April 2026

The Arbiter,

Having seen the Complaint[1] made against Foris DAX MT Limited relating to its alleged failure to stop the execution of several transfers of digital assets to two fraudulent external wallets involving self-hosted addresses[2] despite the introduction of the Travel Rule requirements under Regulation (EU) 2023/1113 (*on information accompanying transfers of funds and certain crypto-assets and amending Directive EU 2015/849*) ('Transfer of Funds (Recast) Regulation' or 'TFR Recast').

The TFR Recast was published in 2023 and, in the case of crypto-asset service providers, is applicable from 30 December 2024.

[1] Page (P.) 1 - 7 and attachments from P. 8 - 42

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

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

1. It was the sole platform through which the scammers operated, meaning that their (Crypto.com brand name of Foris) services are being actively used by criminal entities.

2. Despite reporting the scam and providing detailed proof, there has been no tangible effort to resolve the issue or recover the funds.

3. The current stance of refusing reimbursement or thorough investigation into the matter is not acceptable, particularly given the extent of the loss.

Complainant claims he made the following asset fiat currency transfers sourced from his Italian bank account to the account of Foris:

DATE	**AMOUNT IN €**	**REFERENCE**
06.03.2025	20	p. 49
07.03.2025	232	p. 49
07.03.2025	38	p. 50
09.03.2025	10,000	p. 51
09.03.2025	13,000	p. 52
09.03.2025	10,000	p. 53
09.03.2025	1,699	p. 55
10.03.2025	14,050	p. 56
10.03.2025	600	P. 57
Total	**49,639**	

These payments have been acknowledged as received by Foris and broadly match the compensation sought by Complainant of €49,636.[3] In the police report,[4] there is reference to a loss figure of €49,800 but the Arbiter relies on the amount confirmed received by Foris and confirmed by Complainant as the compensation he is seeking.

The payments originated from Complainant's bank account with UniCredit in Catania to Complainant's account with Revolut and from there to Foris.[5]

From the reply of Foris (referred to later), it is confirmed that these Euro transfers were immediately converted to digital assets and transferred out to two external non-hosted wallets between 07 and 10 March 2025. Overall, the transfers amounted to 0.010309 BTC (Bitcoin) and 51989.62 USDT.[6]

First hearing

At the first hearing held on 16 September 2025, the Complainant, after further elaborating on how he was scammed, reaffirmed his expectations for full compensation from Foris, referring to Travel Rule obligations as follows:

"***I've seen a few cases against Crypto.com on the OAFS website, the last one being uploaded just a few days ago. They are very similar to mine, but with one exception. Those happened before the year 2025. My case happened in March 2025, when the new European regulations were already in force.***

First, we have under the MICA regulations, 2023-11-14, Article (?) which states that since January 2025, Crypto.com and all crypto service providers are required to have robust systems to detect suspicious transactions, act fairly and protect their clients.

Allowing over €48,000 to leave my account in such a short period of time to new and risky recipients without any alerts shows a failure to comply.

[3] P. 3
[4] P. 84
[5] P. 79
[6] USDT known as Tether is *'a stablecoin that is pegged to the U.S. dollar, designed to maintain price stability in the volatile cryptocurrency market by being backed by Tether's dollar reserves'* - https://www.investopedia.com/terms/t/tether-usdt.asp

Second, under the EU Travel Rule, Regulations 2023-11-13, Crypto.com had an obligation to collect and transmit full beneficiary information for crypto transfers.

These rules seek to trace and prevent transfers to fraudsters.

If it had been properly applied, the red flag would have been clear, and maybe I could have saved the situation.

The fact that this transfer went through without any intervention and receiving a standard template reply from Crypto.com, stating that the wallet address was not registered or part of Crypto.com's system, and the users are solely responsible for the transaction, is such a breach of duty.

So, unlike all the other complaints where these rules were not yet enforced, in my case, they were already applicable and binding.

I was a victim of deception. I reported immediately. I acted in good faith. The company, however, failed to act under the new obligations they had in place at that time.

Therefore, I respectfully request that the Arbiter recognizes that the new MICA regulations and the travel rules were already enforced in March 2025, which is when my fraud happened; considers that Crypto.com did not meet the regulations and consumer protect duties and uphold my complaint fully, and orders the company to reimburse all the losses that occurred to me.

With my final closing statement, I would like to say that this case is not only about regulations, but also about human impact.

I did everything I could, as quickly as I could once I realised that I was defrauded.

So, I respectfully ask you to consider both legal obligations and the human cost when making your final decision."[7]

[7] P. 73 - 74

During cross examination, no reference was made to the Service Provider's obligation under the Travel Rule. These obligations will be analysed by the Arbiter in reaching the adjudication decision.

From the cross-examination[8] of the evidence submitted by the Complainant at the first hearing of 16 September 2025, it resulted that:

- Complainant admitted being duped by the scammers showing immediate strong profits on his investments and this led him to make an investment of almost €50,000 in a matter of days, untypical of the way he had conducted his Crypto.com account since he opened it in 2021.
- Complainant did not remember whitelisting the fraudulent wallets he sent his assets to nor did he remember the warnings which Crypto.com give consistently both at the whitelisting stage and the transfer of assets stage.
- No complaint was lodged against UniCredit as when he raised the case verbally with their chief of office, they convinced him they could do nothing about the issue (presumably because the payments were made to his own account with Revolut).
- Complainant raised a complaint with Revolut who *"did not send a satisfactory reply".*[9]
- Complainant reaffirmed that Crypto.com *failed to comply with its duties under MiCA Regulation (2025) and the EU Travel Rule, which required them to detect unusual activity and collect/verify beneficiary information before allowing the disputed transactions to proceed*.

Service Provider's reply

Having considered in its entirety the Service Provider's reply,[10] where the Service Provider provided a summary of the events which preceded the Complainant's formal Complaint and submitted the following:

[8] P. 75 - 79
[9] P. 78
[10] P. 48 - 60 with attachments p. 61 - 71

1. *Background*

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

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

- That the Complainant became a customer of Foris DAX MT Limited through the Crypto.com App and was approved to use the Wallet on 9 November 2021.

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

2. *Timeline*

The Service Provider provided a timeline for the transactions of the Complainant's account which has been explained in the Table above. They confirmed that between 07 and 10 March 2025 BTC and USDT were transferred to 2 external non-hosted wallets with codes ending ….7YQqa and ….08422.

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

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

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

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

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

'QUOTE

6.2.

Without prejudice to the foregoing and any other terms in these Terms, we assume that any and all instructions received from your Enabled Device have been made by the rightful owner. You are solely responsible and liable for keeping your Enabled Device safe and maintaining adequate security and control of your login and authentication details (including, but not limited to, your username, and password), and shall likewise be solely responsible for any access to and use of the Crypto.com App and the Services through your Enabled Device, notwithstanding that such access and/or use may have been effected without your knowledge, authority or consent. We will not be liable to you for any loss or damage resulting from such access and/or use.

…

7.2. Digital Asset Transfers

…

(b) Crypto.com processes all Digital Asset Transfers according to the Instructions received from you and does not guarantee the identity of any recipient. You should verify all transaction information prior to submitting Instructions for a Digital Asset Transfer to Crypto.com as the Digital Asset Transfer may not be cancelled or reversed once processed by Crypto.com unless Crypto.com decides at its sole discretion that the transaction should

be cancelled or reversed and is technically capable of such cancellation or reversal. You acknowledge that you are responsible for ensuring the accuracy of any Instructions submitted to Crypto.com and that any errors may result in the irreversible loss of your Digital Asset.

…

UNQUOTE'.

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

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

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

Further hearings

During the second hearing of 27 November 2025, the evidence of the Service Provider was presented by Julian Yeung who stated:

"In respect of this case, we can see that the complainant has a history with Crypto.com. But in this case, the transactions which form the subject of the complaint began on the 5th of March, I believe. The transactions in this case really concern 26 withdrawals which he made. The withdrawals were made to addresses which he whitelisted. We will explain the whitelisting process later, but these, nonetheless, were transactions that he made on his own accord to accounts which he had himself whitelisted on the Crypto.com app.

In respect of the whitelisting process, I think we have had previous interactions with the Office of the Arbiter Financial Services as regards what the whitelisting process would entail. But in this specific instance, we can see that the whitelisting process is actually more than what was previously submitted to the OAFS on previous occasions. As the complainant himself has clearly identified, there has been a new set of rules which have been put in place since 2025. I believe it is actually the 30th or the 31st of 2024 when these rules were put in place. Nonetheless, for these transactions, what is required is that during the whitelisting process for these wallets, the user of the app has to indicate who is the owner of the wallets, the address, as well as the wallets have to be then reselected when the withdrawal is made.

I appreciate that this evidence has not been put across in the initial filing for the service provider, but we can provide these as quickly as we can after the hearing today ends. Nonetheless, in respect of the transactions, the 26 withdrawals which are in question, we can see that the complainant himself has authorised the withdrawals to go to either a wallet that he claims to be owned by himself or a wallet that he claims to be owned by a Mr. H. The wallets were whitelisted, and the information was collected pursuant exactly to the Travel Rule when the wallets are added to the system. In addition to collecting this information, the users of the Crypto.com app, including the complainant, are warned at least twice again of the need for them to be sure to whom these transactions are going, the veracity and the factualness of the counterparties who are receiving these monies before each and every transaction.

So, once again, we have a situation where the warning is put across to the users when they first add the wallet to the whitelisting list, as well as before each and every one of these transactions. In this respect, we would submit that the transactions made by the complainant himself were to the wallets which he had himself indicated. The service provider is merely carrying out the transactions as he himself has set out. The service provider has also collected the necessary information in compliance with the Travel Rule at the time the wallet is added and, therefore, before each and every one of these transactions is made.

On the basis of that, there is no reason for us to suspect the transactions in this situation. We would also add that the information provided by the complainant is provided to us by himself. We can see that the requisite information has been provided in respect to these transactions.

Finally, we would also add that in addition to the requirements required of us under the Travel Rule, the normal transaction monitoring of these accounts also proceeds in its normal function. We would say that in respect of all these withdrawals which were made, the transactions and the wallet addresses that were identified and supplied by the complainant were not highlighted by us or our external vendors as being a flagged address for any illicit activity. That is to say that there were no warnings that these addresses which the user has interacted with were ones that had been tagged or recognised by the community in general or Crypto.com itself as a wallet address that had been indicated as active or a participant in scam activity.

So, we would refuse his request and accordingly, we believe that the complainant's complaint should be dismissed on those grounds. Thank you."[11]

On cross-examination, it resulted that:

Only some of the transfers were done to a non-hosted wallet which was declared as owned or controlled by the Complainant. Many transfers were made to a non-hosted wallet which the Complainant had declared that it belonged to Svenson He, being the name of the scammer declared by Complainant in his Complaint.

Julian Yeung confirmed that through the various warnings given at the white-listing stage, at the transfer stage and declaration of who was the beneficiary of the recipient wallet (partly being Complainant himself and partly being Svenson He), Foris were in full compliance with their obligation under the MiCA and the Travel Rule.

The Arbiter requested Foris to present evidence of the warnings given as referred by Julian Yeung in his evidence and copies of the declaration made by Complainant as to the beneficiary of the transferee non-hosted wallets.

[11] P. 120 - 121

From the evidence submitted, the Arbiter built the following Table explaining how the digital assets were transferred to non-hosted wallets:

DATE	Wallet ending	Named beneficiary	Asset type BTC	€	Asset type USDC	€	Ref. p.
07.03.25	7YQqa	Complainant	0.002611	217			50; 146
07.03.25	08422	Svenson He			115.43	108	145
07.03.25	"	"			129.37	122	144
07.03.25	"	"			146.24	138	143
07.03.25	"	"			40.64	39	142; 51
07.03.25	"	"			1.71	2	141
08.03.25	"	"			105.48	100	140
08.03.25	"	"			117.12	110	139
08.03.25	"	"			130.25	123	138
09.03.25	"	"			10003.81	9383	137; 51
09.03.25	"	"			13065.55	12255	136; 52
09.03.25	"	"			1467.25	1377	135;
09.03.25	"	"			10500	9851	134;54
09.03.25	"	"			146.45	137	133;54
09.03.25	"	"			1797.3	1686	132;55
09.02.25	"	"			10.58	10	131
10.03.25	"	"			13035.63	12231	130; 56
10.03.25	"	"			1940.19	1820	129;57
10.03.25	7YQqa	Complainant	0.008097	600			128;58

Final Submissions

In their final submissions, the parties largely reiterated their positions as explained in the Complaint, the reply and the evidence during the hearings.

Having heard the parties

Having seen all the documents

Considers

Complainant's profile

The Complainant is a well-educated Italian citizen who has had an account with the Service Provider since 2021, although he made little use of it until the events of March 2025 which are the subject of this Complaint.

Background about the Scam

He fell victim to this scam attracted by high returns he believed he was generating and admitted that he should have seen the red flags but, unfortunately, he did not and he regrets it.[12]

The Arbiter has no reason to doubt the veracity of the Complainant's claims and is satisfied, even on the balance of probabilities, that the Complainant was a victim of a scam. No reasonable doubts have been raised or emerged to the contrary. Consideration has been given to various factors, including: the nature and credibility of the events outlined in the Complaint and the ensuing proceedings; the solemn declaration of the Complainant, testimony and evidence produced; the communications with the scammer;[13] the report/ initiation of criminal proceedings made by the Complainant dated 16 March 2025.[14]

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

[12] P. 76
[13] P. 29 - 40
[14] P. 84 - 86

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.[15]

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

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

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

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 normally 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.

Such 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

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

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"*.[16]

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.

[16] As argued by the Service Provider p. 165, para. 26

As also outlined above, **the Arbiter may 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.[17] 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[18] 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…"*[19]

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.[20] It remained similarly subject to the same principles and requirements under the MiCA regime.[21]

[17] 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.'*

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

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

[20] 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.'

[21] 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.

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 (EBA/GL/2024/11) issued by the European Banking Authority ('EBA') in July 2024[22] ('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."*[23]

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.[24]

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

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

> *"If such information[25] cannot be retrieved via technical means, the originator's CASP and the beneficiary's CASP should obtain that information directly from its customer…".*

The Arbiter has recently decided a case bearing reference number 062/2025[26] where he gives detailed analysis of a Service Provider's (being the same as in this case) obligations under MiCA and Travel Rule especially concerning transfers to non-hosted wallets which are declared as belonging to or controlled by the transferor customer of the Service Provider.

The Arbiter will not repeat his analysis of case 062/2025 as this case has substantially different characteristics which render the protection afforded by MiCA and the Travel Rule not applicable because, as it is evident from the Table of transfers shown above:

1. Most of the transfers were made to a non-hosted wallet of a named third-party beneficiary (Svenson He, the scammer) rather to his own non-hosted wallets.

2. The only 2 transfers where the Complainant named himself as beneficiary of the transferee non-hosted wallet were for amounts under €1,000, which is the minimum level at which the obligations of the transferor CASP kick in under MiCA and Travel Rule.

Causal Factor

The Arbiter has also considered whether the Service Provider had an obligation to query the sudden surge of transactions going through his account in March 2025 which was totally incongruous with the quasi-dormant pattern of activity on his account in the previous four years.[27]

[25] Per para. 77 of the Guidelines, being information necessary to determine whether or not a recipient wallet is a self-hosted wallet (external wallet)
[26] https://financialarbiter.org.mt/sites/default/files/oafs/decisions/2706/ASF%20062-2025%20-%20KJ%20vs%20Foris%20DAX%20MT%20Limited.pdf
[27] P. 74; 116 -118

In the context of crypto markets that should be the preserve of educated investors, and in the context of a market where Bitcoin had dipped from its peak above USD100k reached in December 2024 to some USD 84k at the time of these events (before peaking again to nearly USD122k in October 2025), a sudden surge in turnover for an amount of some €50k is not necessarily a reason for a CASP to suspect fraud and trigger enquiries with their customer.

This is more so in the case where the customer had been dealing moderately in crypto assets for some four years. Any AML issues related to such surge are beyond the role of the Arbiter.

Furthermore, although the Arbiter notes that Complainant stated he does not remember the pop-up warnings given at the whitelisting and transfer stages as explained in the evidence of the Service Provider (copies of which have been submitted as requested by the Arbiter[28]), the balance of probabilities is that these warnings were duly given but not read with due attention by 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 circumstances, in accordance with the above analysis, the Arbiter is not upholding this Complaint and hereby denies the Complainant's request for compensation for the suffered loss.

The Arbiter considers that the Complainant cannot expect to shift blame for his loss, primarily caused by his own greed and negligence onto the Service Provider, seeking refuge under the MICA and Travel Rule mechanisms which entered into force in 2025, and which are not applicable to the particular circumstances of his case.

[28] P. 153 – 155; 169 - 173

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.