Before the Arbiter for Financial Services

Case ASF 153/2024

TZ

('the Complainant')

vs

Foris DAX MT Limited (C 88392)

('Foris' or 'the Service Provider')

Sitting of 18 August 2025

The Arbiter,

Having seen **the Complaint** dated 1 August 2024[1] relating to the Service Provider's alleged failure to prevent, stop or reverse the payment in crypto of Bitcoin (BTC) made by the Complainant himself from his account held with *Crypto.com* to an external wallet allegedly owned by third parties who could be fraudsters or connected to fraudsters.

The Complaint

The Complainant opened an account with the Service Provider on 26 February 2024. Between 9 and 27 March 2024, he carried out multiple transactions involving transfer of fiat currency amounting to approx. €80,000.

On each occasion, the funds were immediately converted to BTC and transferred out to the external wallet.

The funds were transferred from his account with Bank of Austria[2] and were received into his account with Crypto.com as follows:

[1] P. 1 - 6 and attachments p. 7 - 39
[2] P. 74

Date	Amount in euro	Reference
29.02.2024	15,000	p. 46
12.03.2024	5,400	p. 47
18.03.2024	10,700	p. 48
21.03.2024	10,700	p. 50
27.03.2024	42,000	p. 51
TOTAL	**83,800**	

Following conversion into BTC, there were ten withdrawals of BTC to the external wallet involving a total transfer of 1.224936 units. Five of these purchases occurred on 27.03.2024 when the 0.56 BTC bought with the last transfer was broken down into smaller pieces as instructed by the fraudsters guiding the Complainant when he reported that the Crypto.com system was blocking him from sending the units bought in one transfer.[3]

The Complainant stated that:

'Crypto.com did not prevent me from sending my Bitcoin to a scam wallet and did not respond when I sent €40,000 within a very short time (within 1 day) to a crypto.com scam wallet. I am of the opinion that crypto.com knows that this is a scam wallet. They didn't warn me or offer me any support. I think it's only fair for the blockchain system because I know where the funds are that if I report and report a fraud, a platform has to react and provide complete support to clear up the fraud and help stop it. This is subject to the so-called compliance rules.'[4]

…..

'I clearly informed crypto.com when and in what amount I sent money from crypto.com to a fraudulent wallet. I also sent my report, which I filed in Austria for serious fraud (approx. €80,000) to crypto.com. I also sent the different wallets that I found after researching with friends. Since the crypto.com system is transparent with the help of the blockchain, there is no obstacle to checking

[3] P. 8
[4] P. 2

these fraudulent wallets. At least it would have to be possible to freeze the Bitcoin in order to initiate an investigation. However, crypto.com refuses any further investigation, says they are not responsible and cannot and/may not do anything, and is waiting for pressure from "above".'[5]

Complainant requested a full investigation of his transfers from his Crypto.com wallet to the fraudulent wallet and a refund of BTC 1.224936 units valued approximately at €79,500.[6]

When the Arbiter asked him whether he is seeking as compensation the BTC units or €79,500, the Complainant stated he was demanding compensation for €79,500.[7][8]

In his original complaint directly to Service Provider, he had stated:

'*This letter is to inform Crypto.com about the fraudulent activity that has been performed by the fraudulent company named "Tradingarena247" starting in February 2024. Please note that, due to the fact that such a malicious fraud took place utilizing your services, I do consider Crypto.com to be directly involved in it.*

As was stated previously, I fell victim to the online scam, which misrepresented themselves as legitimate brokers offering me to make profits on so-called "online trading" without any risk. I thought I was going on with a legitimate investment track, so I would like to mention that their methods were illegal, manipulative, non-regulative, and very questionable. As a consequence, the fraudsters have maliciously utilized Crypto.com's services in order to steal all my hard-earned funds, a total amount of ***1.224936 BTC.***

I would like to emphasize the fact that I couldn't make a conscious decision as I was misinformed from the beginning as to the nature of the fraudsters, meaning I couldn't have known that these transactions are risky. I was never contacted by your employees, nor was I provided with adequate warnings or alerts from your

[5] P.3
[6] P. 3
[7] P. 73
[8] Following closure of proceedings and final submissions, Complainant sent an email dated 19.07.2025 (not in the proceedings) changing his request to refund of the BTC which given its price escalation to nearly US$120k per unit would give him a substantial gain over the funds 'invested'.

side, although those transactions must have raised concerns (I have fully explained them below).”[9]

Reply of Service Provider[10]

In their reply of 13 August 2024, Service Provider explained that Foris offers the following services:

‘Background

- *Foris DAX MT Limited (the “**Company**”) offers the following services: a crypto custodial wallet (the “**Wallet**”) and the purchase and sale of digital assets through the Wallet. Services are offered through the Crypto.com App (the “**App**”). The Wallet is only accessible through the App and the latter is only accessible via a mobile device.*
- *Our company additionally offers a single-purpose wallet (the “**Fiat 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.*
- *Mr … (the “Complainant”), e-mail address … … … ... became a customer of Foris DAX MT Limited through the Crypto.com App and was approved to use the Wallet on 26 February 2024.*
- *The Company notes that in the submitted complaints file, (the Complainant) has outlined his desired remedy as: (i) reimbursement for incurred financial losses.”*[11]

They gave a detailed sequence of the various transactions executed by the Complainant on his wallet.[12]

They concluded that:

[9] P. 25
[10] P. 45 - 54 and attachments p. 55 - 65
[11] P. 45
[12] P. 46 - 52

'In summary, (the Complainant0 has withdrawn the total amount of 1.224936 BTC from his Crypto.com Wallet towards an external wallet address between March 9, 2024 – March 27, 2024.

The wallet address in question is:

183qMFaL2yEM1xQJjC1FAPbQFA5zeUtYES

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

While we sympathize with the Complainant and recognize that he may have been misled or induced into transferring funds to an alleged fraudster, it is important to note that these transfers were made solely at the Complainant's request. We must also emphasize that the address the funds were transferred to, does not belong to the Company and as such, any due diligence of the ownership of this address falls under the responsibilities of the provider of said wallet.

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

(The Complainant) is solely responsible for the security and authenticity of all instructions submitted through his Wallet as outlined in the Foris DAX MT Limited Terms of Use.

Please see the relevant section of the Terms of Use for your reference.

QUOTE

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

In summary, it seems conceivable that the Complainant has been the victim of an alleged scam. However, due to the nature of the external wallet and the fact that it is not hosted or operated by Foris DAX MT, we can neither confirm nor deny this.

Whilst we fully empathize with (the Complainant) in this regard, it cannot be overlooked that he had willingly, transferred his virtual asset holdings from his Crypto.com Wallet to an external wallet address which he nominated.

As outlined above in the Foris DAX MT Limited Terms of Use, the Complainant is solely responsible for the security and authenticity of all instructions submitted through the Crypto.com App, and as such, the Company cannot accept liability for the veracity of any third party or for the instructions received from the Complainant themselves."[13]

Hearings

During the first hearing held on 16 April 2025, Complainant said:

'***I think that Foris DAX MT Limited sent my money to a fraudulent wallet.***

According to the European Union Regulation (EU) 2023/1113, they are not allowed to do that. I say that this regulation is in force, and they have to abide with this regulation in this case.

Therefore, I think that they have irregularly transmitted my cryptos to a fraudulent wallet.

I say that on 27 March 2024, they monitored my transaction, and they did not transact it two times and then I split it into four parts and, then they let it go.

[13] P. 52 - 53

So, they knew and a day later, they sent me an email where they said that this was a fraudulent wallet because they monitored my transaction.

I say that I really did not know that this was a fraudulent wallet because I believed that this was someone that I knew very well who is an expert in financing, and some fraudulent people stole his identity.'[14]

On being cross-examined, he said:

'It is being said that in my complaint I say that 'Crypto.com did not prevent me from sending my Bitcoin …'.

Asked whether it is correct to say that it was my choice to actually invest in Bitcoin with Tradingarena247, and that it was me who authorised the payments, I say, yes, it was me, but I am going on your platform, in your Bitcoin system, in the cryptocurrency system, and you are responsible for that. What is going on? It is like going to my bank. I make the transaction and the bank is responsible for the money that goes there.

I confirm that I chose to send the money to Tradingarena247.

I say that my money left the bank account in Austria and sent to Crypto.com. I sent the money from my bank to Crypto.com. At Crypto.com, I bought Bitcoin and I sent the Bitcoin to the scammer's wallet.

My money was in an account at the Bank of Austria.

Asked whether I raised a complaint with my bank with regard to the transfer of my money from the bank account to Crypto, I say, yes, but they did not make any mistake because they said that they have to see the rules and the rules say, from where does the money come from and where does the money go to. And the money comes from me. At the bank, they have known me for a very long time; I have a business and I have a private account. So, they know that I have money; so, they sent my money (and that's no problem) to Crypto.com. And Crypto.com is a platform, it is a company, stationed in Malta, and everything is OK, so, my bank is not the case. The case is the irregularity of what we have got here.

Asked by the Arbiter whether I have raised an issue with my bank in Austria why they did not stop me from sending this money to Crypto.com, I say, no. Why do they have to? I say, no. I did not raise an issue with the bank why they did not

[14] P. 72

stop me from sending this money to Crypto.com. I confirm that I did not file a complaint with my bank.

I confirm that my bank knew that I was sending money to Crypto.com and they did not stop me; and although they did not stop me, I did not file a complaint with the bank.

Asked whether Tradingarena247 was a platform which I found myself, I say that I went to a platform, it was called Trade Service, and then, I had a discussion with them and they guided me at the start to Crypto.com, how to buy cryptos and that I had to send them to the trade. And this was a man called Thomas (?). I made a wallet. This Trade Service guided me all the way. And then they said that I have to look at Tradingarena247 to see how big my amount is. I saw, and I said OK. And the last time I sent money to them, I wanted to have my money, and they said I have to pay something like taxes. And this was €40,000. I wanted to pay €40,000 at once. I think it was 0.62 Bitcoin at that time. I wanted to pay it at once and that was on the 27th. And it was stopped twice. And, then Trade Service guided me to split it into four parts and that is what I did. And, then I sent €10,000 three times and Crypto.com made the transaction. On the fourth time, they stopped it. And, then I made two more payments of €5,000 each and they let them go.

On the next day, I think I sent Crypto.com a letter and they wrote back that I had sent money to a scammer wallet.

So, if I sent money to a scammer wallet, you have to break down the connection. You are not allowed to send the money. It is in the old regulation of 2015. I think Crypto.com knows the regulations.

Asked in what manner I communicated with Tradingarena247, I say that the Trade Service was on a Telegram channel. I made a link there and then I was on the Trade Service. The Trade Service communicated with me and guided me all the way. I say that I sent to only one wallet. All the payments were made to the same wallet. Then the Trade Service told me to make an account at Tradingarena247. I did that, he guided me through that and then I say my money account there. He showed me how much money I had there.'[15]

During the second hearing on 4 June 2025, Service Provider submitted:

[15] P. 73 - 75

'I think that, for the record, it's important to state that (the Complainant) became a user of the service provider on the 26 February 2024; and the dispute at hand revolves around a series of withdrawals which occurred from 9 March 2024 to 27 March 2024. I think there is no dispute that (the Complainant) himself authorised these transactions himself. I think the question now only surrounds the service provider's responsibility, if any, regarding these transactions as well as the nature of the withdrawals at hand.

So, I think it's important for us to keep in mind the number of steps that the user has to take in order to withdraw any crypto assets or digital assets on our platform. Firstly, he must add the withdrawal address to his wallet. It's what we call whitelisting.

Crypto.com provides the service whereby a 24-hour lock is placed on a new address that is whitelisted for users to opt into. On this occasion, we can see that (the Complainant) did not opt into this protection service. This protection service would have meant that he would not be able to withdraw any cryptocurrency within the first 24 hours of adding this external wallet to his address. It's also important to keep in mind that, at all times, there is only one wallet address in question to which withdrawals were made to, and this is a wallet that's not hosted by Crypto.com. So, that's to say that we do not have any information as to who the user is as well as any sort of particulars as to the person's identity.

Now, upon adding a new address to the Crypto.com account, a warning is given to each and every user each and every time they add a new address; it warns them that they should be careful what addresses they add as whitelisted addresses or withdrawals. We specifically warn users that there are platforms that promise high returns; unrealistic ones, we might add. There is a reference to the wallet belonging to someone whom you trust. And, also, a reference to an article posted by Crypto.com which is constantly updated which features the usual scam patterns for such activity. We invite the user to click on this link to learn more, but we do warn them specifically that they should be wary of withdrawing funds to platforms that promise them unrealistically high returns.

All this is done at the whitelisting stage. Now, the whitelisting stage is separate to the withdrawal stage and at the withdrawal stage of each and every transaction, a similar warning pops up yet again to remind the users not to withdraw to these sorts of platforms, particularly platforms which promise unrealistically high returns or belonging to people whom they don't have

absolute trust in. And, again, we ask the users to review the scam document so that they are able to educate themselves as to the common factors and scam tactics out there that malicious third parties are perpetrating.

Now, finally, in each of these situations, both at the whitelisting stage as well as the withdrawal stage, we warn the users that transactions of cryptocurrency are immutable. That's to say they cannot be reversed and that they are to take responsibility for their withdrawals pursuant to both that warning as well as the Crypto.com terms and conditions offered by each and every service entity, including DAX MT.

So, the path by which any user has to commit a withdrawal to a wallet, he is warned firstly at the stage at which they add the address and then warned again at each and every withdrawal.

So, I understand, Mr Arbiter, we haven't provided these screenshots for your consideration and, if you will allow us to do so to support our current oral evidence, we can provide you with screenshots to show you what exactly those warnings look like.

Now, as to the final set of transactions which (the Complainant) has executed, we would firstly say that there is no evidence on our end to indicate that the withdrawal address was linked to any scam activity at the time of these transactions. There's nothing to suggest that the transactions which were performed were to a wallet which we had identified or was identified by our vendors as being a scam wallet. In fact, if you look at the wallet today (and this is open evidence that anyone can look at themselves), there seems to be much activity with this wallet yet. That would suggest that this wallet is still active and participating across the blockchain.

Now we can see that there were a number of transactions which were titled as 'cancelled' in our transaction history. All we can say is that we do not know the reason for this. It suggests that there were technical difficulties in the carrying out of the transaction, but this is not to say that the wallet address had been added to any blocked lists. If a wallet is added to our blocked list at the time of these transactions, you are unable to process the transactions whether or not the amount is large or small. Now a further indicative factor in this situation is that the warning to (the Complainant) was not sent to him until some 16 hours after the transactions first occurred. Now, 16 hours would be quite a long time for us to acknowledge that a transaction had happened as a matter of a scam.

Instead, what happens is that on a regular basis, (I believe it's usually within the 48 hour/24 hour cadence; I can't be sure) we are invited and updated by our external vendors as to suspect addresses which have occurred or addresses which have been linked to scam activity.

From the timing of the email which was sent, which was quite some time after the last of these transactions, we would suggest that, unfortunately, it was only identified that this wallet was involved with scam activity after the last of these transactions had occurred. In fact, (the Complainant) himself did not contact us to ask to reverse these transactions until 21 May 2025. So, what we're saying is that Crypto.com took the initiative to warn him that the wallet which he had interacted with had them linked to a scam. We did not identify that until the time of the email, which is a number of hours, quite a number of hours after the last of these transactions. The reason why the transactions were so-called 'cancelled' is due to a technical fault as opposed to a block on any sort of withdrawal or any link to any scan pattern at the time of the transactions as can be evidenced by the fact that he was successfully able to carry out transactions of a smaller nature just a number of minutes after he attempted the first ones.

So, all in all, we would say that the service provider has taken all necessary steps and all required steps to ensure that clients are transacting safely and responsibly. We have warned the user that at the point at which they add these addresses to both their white list as well as when they carry out the transaction, they should be wary of carrying out transactions with these and hosted wallets. We have warned them that transactions are irreversible, and we rely also on the terms and conditions provided by us in providing the services of the app to the user.

All in all, we would say that we do not have any responsibility for these transactions and as such, we will not be processing, and we have not processed a refund to the complainant. So that's the evidence of the service provider.'[16]

On cross-examination, Foris representative stated:

'It is being said that the last transaction happened on the 27 March 2024, and now in my evidence I said that the complainant contacted Foris DAX and told them about the complaint officially on 21 May 2025. Asked whether he

[16] P. 76 -79

contacted me in 2025 or 2025, I say, it was in 2024, two months after the last transaction.'[17]

When Complainant asked the Foris representative whether he agrees that EU Regulation 2023/1113 was in force at the time of these transfers, the representative of Foris stated:

'Mr Arbiter, I think we will address these in the submissions, but I will point out that Article 39 of that regulation states that the regulations that (the Complainant) is citing, whether or not they are applicable to this case, did not come into force as applicable law until 31 December 2024. So that was the number of months after these transactions.'[18]

The Arbiter then asked clarification as follows:

'There was a point in time, where (the Complainant) was trying to make a transfer of a big amount and, for some reason, this did not go through. The Arbiter is not too sure whether this did not go through because he cancelled it or because there were technical problems. But then, apparently the fraudsters told him that if he breaks it into smaller pieces, it will go through. And, actually, that happened with the difference that the last one had to be broken into even smaller pieces.

The Arbiter asks the complainant whether he tried to do the transaction, and he cancelled it to break it in smaller amounts or he tried to do it and he was not allowed to do the transaction.'[19]

Complainant replied:

'I did not cancel it. It did not go through. Normally, every transaction goes through, and it was the first time that it did not go through. And I tried it two or three times and it did not go through.

Asked by the Arbiter when it didn't go through, whether I cancelled it and made a smaller transfer, I say, no, I didn't cancel it. No, I didn't even cancel it. I tried it again because the fraudsters told me that I have to split it but I did not cancel it.'[20]

[17] P. 79
[18] *Ibid*.
[19] P. 81
[20] *Ibid*.

The representative of Foris stated:

'No. There was a technical problem; that is what we have gathered.

What I can explain is that if a transaction is deemed to be of a suspicious nature, that would mean that the withdrawal address is blocked. What we can see from the case at hand is that the withdrawal address was not blocked. So that suggests that the reason why the transactions were cancelled was because there was a technical difficulty.

I can say that when the withdrawals of the first three sums occurred, they were relatively close in time together. If there is a suggestion that we would block large sums but not small sums, I can say that that's not something that is practised on our platform as far as this case is concerned.

If there is an inkling of a scam, that address would be added to the list of addresses which are blocked for transactions occurring from Crypto.com.

So, what I can say on this case is that it does not appear that there was any suspicion of scams, and that is backed up by the fact that the email which alerted (the Complainant) to any suspicion only came quite some time after the last of these transactions occurred.'[21]

Final Submissions

In his final submissions, the Complainant basically admitted that out of ignorance and stupidity,[22] he had disregarded all warnings given to him by the Service Provider at the time of whitelisting the external wallet and at the time of making each transfer.

He again maintained that the fact that his last payment on 27 March 2024 could not go through as a single shot but had to be broken down into five smaller payments was strong indication that something was wrong with the external wallet and that the Service Provider already had knowledge that it was being used for scamming victims and should have stopped the payments. Instead, he received a warning only the next day reporting Crypto.com's suspicion about the

[21] P. 81 - 82
[22] P. 84

external wallet he had used being *associated with malicious activity and controlled by scammers.'*[23]

He further maintains that such warning rather than block all payments to the suspicious wallet limited the weekly transfers to US$20,000.

He asks how if the external wallet was suspicious, one would still allow transfers up to US$20,000.[24] [25]

In their final submissions, Service Provider provided evidence (as requested and authorised by the Arbiter) of the warnings given to Complainant at the time he was whitelisting the external wallet and at the time he was making each and every transfer thereto.[26] In spite of such warnings, the Complainant confirmed that ***'Yes, I trust this address'***[27] at the whitelisting stage and ***'Confirm and Withdraw'***[28] at every transfer stage.

They also reaffirmed that at the time of making the transfers, they had no knowledge or awareness that the external wallet was associated with any fraud or scams, and they only gained such awareness after the last transfer was executed leading to the warning of 28 March 2024.

They also confirm that they abide by all regulatory requirements including AML and that the provisions of EU Regulation 2023/1113 were not effective at the time of the transfers as such rules only kicked in on 30 December 2024.

Consequently, they reaffirmed that it was the Complainant through his gross negligence that was responsible for his loss.

Analysis and considerations

Having heard the parties and seen all the documents and submissions made,

Further Considers:

[23] P. 88
[24] *Ibid*.
[25] The notice limits transfers up to US$ 20K to 'external crypto withdrawals and transfers' not to the specific wallet. In their evidence, Service Provider stated that once an external wallet was reported suspicious, all transfers thereto, irrespective of amount, are blocked – p. 82
[26] P. 96 - 99
[27] p. 96
[28] P. 97

The Merits of the Case

The Arbiter is considering the complaint, and all pleas raised by the Service Provider relating to the merits of the case together to avoid repetition and to expedite the decision as he is obliged to do in terms of Chapter 555[29] which stipulates that he should deal with complaints in '*an economical and expeditious manner'.*

The Service Provider

Foris DAX was at the time of these events licensed by the Malta Financial Services Authority ('MFSA') as a VFA Service Provider as per the MFSA's Financial Services Register.[30] At the time of the transfers subject of this complaint they had a Class 3 VFAA licence granted, on 16 April 2021, by the MFSA pursuant to Article 15 of the Virtual Financial Assets Act, 2018 ('VFAA').

As per the unofficial extract of its licence posted on the MFSA's website, the Class 3 VFAA Licence authorises Foris to provide the following VFA Services: (i) Execution of orders on behalf of other persons (ii) Dealing on own account and (iii) Custodian or Nominee Services to Experienced and Non-Experienced investors.[31]

As outlined in the disclaimer section of the *Crypto.com* website, Foris is *'trading under the name 'Crypto.com' via the Crypto.com app'*. [32]

Observations & Conclusion

Summary of main aspects

The Complainant made the transfers of his digital assets subject of this complaint using the *Crypto.com* app. The said transfers were made to external wallet addresses thinking the wallet belonged to him as his investment account with *Tradingarena 247* which later he discovered were scammers. The transfers to the external wallets were made on the specific instructions of the Complainant. External wallets are recognised only by their number and their proprietors or

[29] Art. 19(3)(d)
[30] https://www.mfsa.mt/financial-services-register/
[31] https://www.mfsa.mt/financial-services-register/
[32] https://crypto.com/eea/about

beneficial owners are not known to the transferor. The Service Provider had no obligation under the regulatory regime applicable at the time of the transfers to keep or make available information relating to external wallets.

Complainant maintained that EU Regulation 2023/113 of 31 May 2023[33] was already effective. This Regulation substantially increases the responsibility of the Service Provider to ensure that the recipient wallet is under the control of their remitting client. However, Article 40 of this Regulation clearly states that the Regulation was to enter into force on 30 December 2024, that is well after the date these transfers were executed. In fact, the EBA Guidelines for the execution of this regulation were issued on 4 July 2024[34] and these again restate in the Executive Summary page 3 that *"these Guidelines will apply from 30 December 2024".*

In essence, the Complainant is seeking compensation from Foris for their failure to prevent, stop or reverse the payments he made to the fraudster on the basis that the Regulation and Guidelines above referred to were already effective when, clearly, they were not when the transfers subject of this complaint actually occurred.

The Complainant *inter alia* claimed that the services provided by Foris were not correct given that it transferred the assets but failed to protect him from fraud and allowed their infrastructure to be used for fraudulent purposes. He also argued that the fact that he had to breakdown the transfers into small tranches and that he received notification about the fraudulent nature of the external wallet less than 24 hours after the last transfer was executed, indicate that the Service Provider should have known that the wallet was being used for fraudulent purposes.

On its part, the Service Provider is, in essence, claiming that it has no responsibility for the payment done by the Complainant as he himself had to verify the transaction information (as per the provisions of the *Crypto.com App Terms of Use*) and that it was not possible for Foris DAX to revoke or reverse the crypto withdrawal once the transaction was done on the blockchain.

[33] https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32023R1113
[34] EBA/GL/2024/22 Travel Rule Guidelines

They deny that they had any warnings about the fraudulent nature of the external wallet and, also, deny that the problem with having to break the last transfer in small tranches had anything to do with any such knowledge or warnings.

Applicable Regulatory Framework

As outlined above, Foris DAX was at the time the holder of a Class 3 VFAA licence granted by the Malta Financial Services Authority ('MFSA') under the Virtual Financial Assets Act, 2018 ('VFAA').

Apart from the relevant provisions under the VFAA, and the *Virtual Financial Assets Regulations, 2018 (L.N. 357 of 2018)* issued under the same act, Foris DAX is also subject to the rules outlined in the Virtual Financial Assets Rulebook ('the VFA Rulebook') issued by the MFSA. The said rulebook complements the VFAA by detailing *inter alia* ongoing obligations applicable for VFA Service Providers.

Chapter 3 of the VFA Rulebook specifically includes the rules applicable for VFA Service Providers which such providers must adhere to.

The Arbiter further notes that in the year 2020, the MFSA has also issued a *'harmonised baseline guidance on Technology Arrangements'*[35] applicable to its licence holders (including under the Virtual Financial Assets) titled *'Guidance on Technology Arrangements, ICT and Security Risk Management, and Outsourcing Arrangements'* ('the Guidance').

The FIAU[36] also issued Implementing Procedures on the Application of Anti-Money Laundering and Countering the Funding of Terrorism Obligations to the Virtual Financial Assets Sector.[37] Section 2.3 of these Implementing Procedures detail the monitoring and transaction records obligations of VFA licensed entities.

Further Considerations

Having considered the particular circumstances of the case, including the submissions made and evidence provided, the Arbiter considers that there is no sufficient and adequate basis on which he can uphold the Complainant's request

[35] Guidance 1.1.2, Title 1, *'Scope and Application' of the 'Guidance on Technology Arrangements, ICT and Security Risk Management, and Outsourcing Arrangements'*.
[36] Malta's Financial Intelligence Analysis Unit being competent authority of AML issues.
[37] Layout 1 copy (fiaumalta.org)

for the reimbursement by the Service Provider of the sum the Complainant himself transferred to an external wallet from his crypto account. At no stage has the Complainant raised any doubt as to his having authenticated the transactions personally.

This is particularly so when taking into consideration various factors, including the nature of the complaint, activities involved, and the alleged shortfalls as further detailed below:

- The Complaint involves a series of payments made by the Complainant from his account held with Foris to allegedly fraudulent external wallets causing a loss to the Complainant of approximately €80,000.

  The Complainant expected the Service Provider to prevent or stop his transactions. He claimed that the Service Provider had an obligation to warn him of potential fraud

  The Arbiter considers that no adequate and sufficient evidence has however emerged to substantiate the claim that the Service Provider could have itself prevented or stopped the transaction on the basis of knowledge or suspicion on the fraudulent nature of the recipient wallet.

  The Complainant admits that he himself 'whitelisted' the address giving all clear signal for the transfer to be executed**.**

  In the process of such whitelisting as well as in the process of the actual transfers, the Complainant was warned by the Service Provider to ensure that he was responsible to keep control over the transferee wallet.[38]

  In fact, the Complainant himself did not raise any suspicion or evidence that there was any link between the Service Provider and the external wallet addresses he himself provided.

- The exchange of fiat currency into crypto and withdrawals from one's crypto account, including withdrawals to an external wallet is, in its own right, part

[38] P. 96 - 99

of the typical services provided to millions of users by operators in the crypto field such as the Service Provider.

- Furthermore, it has not been demonstrated nor emerged that the alleged fraudster, to whom the payment was made by the Complainant, was another *Crypto.com* App user and, thus, a client of the Service Provider in the first place. The transfer was rather indicated to have been done to an *'external wallet'* and hence the Service Provider had no information about the third party to whom the Complainant was transferring his crypto.

- The Complainant seems to have only contacted the Service Provider on 13 May 2024,[39] some 6 weeks after the last of the disputed transactions was already executed and finalised.[40]

  Once finalised, the crypto cannot be cancelled or reversed as specified in the Service Provider's Terms and Conditions of Use (and as typically indicated on various other internet sites).[41]

  Once a transaction is complete and, accordingly, is not in a pending state, the crypto transaction cannot be cancelled or reversed by the Service Provider as provided for and warned in the Terms and Conditions of Foris.

  As indicated by the Service Provider, Clause 7.2(b) of its Terms and Conditions regarding the use of the Crypto.com App Services specifies that:

  '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 …'.[42]

  On the basis of the facts presented during the case, the Arbiter could not conclude that the Service Provider failed to adhere to any specific obligation, or any specific regulatory requirements applicable to it, nor did he find any

[39] P. 7 - 19 with attachments
[40] Crypto transactions may be processed and completed within a few minutes or hours (as indicated on various websites following a general search on the internet).
[41] E.G. https://www.chargebackgurus.com/blog/chargebacks-more-volatile-complex-than-cryptocurrency
[42] P. 53

infringement of the Terms and Conditions applicable in respect to the service offered.

In arriving at his decision, the Arbiter considered the following aspects:

i. AML/CFT Framework

Further to the Prevention of Money Laundering Act (Cap. 373) and Prevention of Money Laundering and Funding of Terrorism Regulations ('PMLFTR'), the Financial Intelligence Analysis Unit (FIAU) issued Implementing Procedures including on the *'Application of Anti-Money Laundering and Countering the Funding of Terrorism Obligations to the Virtual Financial Assets Sector'*.[43]

These are *'sector-specific Implementing Procedures [which] complement the Implementing Procedures – Part I [issued by FIAU] and are to be read in conjunction therewith'*.[44] Section 2.3 of these Implementing Procedures detail the monitoring and transaction records obligations of VFA licensed entities.

It is noted that the VFA Act mainly imposes transaction monitoring obligations on the Service Provider for the proper execution of their duties for Anti Money Laundering ('AML') and Combating of Financing of Terrorism ('CFT') obligations in terms of the local AML and CFT legislative framework.

Failures of the Service Provider in respect of AML/CFT are not in the remit of the OAFS and should be addressed to the FIAU. In the course of these procedures, no such failure was indeed alleged. The Arbiter shall accordingly not consider compliance or otherwise with AML/CFT obligations in this case.

ii. MiCA and the Travel Rule

As to the identification of the recipient of the funds, it is noted that MiCA[45] and Travel Rule[46] obligations which entered into force in 2025, and which give more

[43] https://fiaumalta.org/app/uploads/2020/09/20200918_IPsII_VFAs.pdf
[44] Page 6 of the FIAU's Implementing Procedures on the *'Application of Anti-Money Laundering and Countering the Funding of Terrorism Obligations to the Virtual Financial Assets Sector'*
[45] EU Regulation 2023/1114 on markets in crypto assets https://eur-lex.europa.eu/legal-content/EN/AUTO/?uri=celex:32023R1114
[46] EU Regulation 2023/1113 https://eur-lex.europa.eu/legal-content/AUTO/?uri=CELEX:32023R1113&qid=1740401464257&rid=1 and EBA Guidelines on Travel Rule https://www.eba.europa.eu/sites/default/files/2024-07/6de6e9b9-0ed9-49cd-985d-c0834b5b4356/Travel%20Rule%20Guidelines.pdf

protection to consumers by having more transparency of the owners of the recipient wallets were not applicable at the time of the events covered in this Complaint which largely happened in March 2024.

The Arbiter shall thus not consider the MiCA provisions and Travel Rule obligations for the purposes of this Complaint.

iii. Technical Note

A Technical Note (issued in 2025) with guidance on complaints related to pig butchering was recently published by the Arbiter. In respect of VFA licensees, the Technical Note states as follows:

> *'Virtual Financial Assets Service Providers (VASPs)*
>
> *VASPs should be aware that with the coming into force of Regulation (EU) 2023/1113 and the Travel Rule Guidelines their obligation to have reliable records on the owners of external (unhosted) wallets increases exponentially as from 30 December 2024.*
>
> *Arguments that they have no means of knowing who are the owners of external wallets which have been whitelisted for payments by their client will lose their force.*
>
> *VASPs have been long encouraged by the Office of the Arbiter (in decisions dating back from 2022),[47] for the devise of enhanced mechanisms to mitigate the occurrence of customers falling victims to such scams.*
>
> *Furthermore, in the Arbiter's decisions of recent months there is a recommendation that VASPs should enhance their on-boarding processes where retail customers are concerned warning them that custodial wallets may be used by scammers promoting get-rich-quick schemes as a route to empty the bank accounts of retail customers and disappear such funds in the complex web of blockchain anonymous transactions.[48]*

[47] Such as Case ASF 158/2021
[48] Such as Case ASF 069/2024

Compliance with such recommendations or lack thereof will be taken into consideration in future complaint adjudications.'[49]

The Arbiter will not apply the provisions of the Technical Notes retroactively.

Hence, for the avoidance of any doubt, the said Technical Note is not applicable to the case in question.

iv. Issue regarding the transfer of 0.65 BTC to external wallet on 27.03.2024 had to be broken down into 5 small tranches[50]

Complainant maintains that the fact that this transfer was refused by Crypto.com's system and, under the guidance of the fraudster, had to be broken down in five smaller tranches to flow through is sufficient evidence to prove that Service Provider must have had warnings on the suspicious nature of the recipient wallet. His suspicion is fortified by the fact that just one day later, Crypto.com informed him that the said wallet was indeed *'associated with malicious activity and controlled by scammers'*.[51]

In his final submission the Complainant takes issue with the action to limit transfers to the external wallet of US$20,000 weekly and questions how Crypto.com could allow transfers of any value to a suspicious wallet.

Service Providers deny that the breakdown of the last transfer into five small tranches was anything but due to technical problems and emphatically deny that it was inspired by any suspicion of fraud associated with the recipient wallet. They also emphasise that once subject to any suspicion, all transfers to such wallet are blocked. The reference to the US$20k limitation of weekly transfers referred to external wallets generally not to the scam wallet specifically.

In the absence of specific evidence to the claims of the Complainant, the balance of probabilities is in favour of the Service Provider's version of events.

[49] Emphasis added by the Arbiter
[50] P. 51 - 52
[51] P. 88

v. Duty of Care and Fiduciary Obligations

It is noted that Article 27 of the VFA Act states:

> *'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 (CAP 16) in so far as applicable**.'*[52]

Article 1124A (1)(a) of the Civil Code (Chapter 16 of the Laws of Malta), in turn further provides the following:

> *'1124A. (1) **Fiduciary obligations arise in virtue of law, contract, quasi-contract**, unilateral declarations including wills, trusts, **assumption of office or behaviour whenever a person** (the ''fiduciary'') –*
>
> *(a) **owes a duty to protect the interests of another person and it shall be presumed that such an obligation where a fiduciary acts in or occupies a position of trust is in favour of another person**; …'*[53]

It is further to be pointed out that one of the High Level Principles outlined in Section 2, Title 1 *'General Scope and High Level Principles'* Chapter 3, Virtual Financial Assets Rules for VFA Service Providers of the VFA Rulebook, that applied to the Service Provider at the time of the disputed transactions in 2022, provides 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.'*

It is also noted that Legal Notice 357 of 2018, Virtual Financial Assets Regulations, 2018 issued under the VFA Act, furthermore, outlined various provisions relevant

[52] Emphasis added by the Arbiter
[53] Emphasis added by the Arbiter

and applicable to the Service Provider at the time. Article 14 (1) and (7) of the said Regulations, in particular, which dealt with the *'Functions and duties of the subject person'* provided the following:

> *'14. (1) A subject person having the control of assets belonging to a client shall safeguard such assets and the interest of the client therein.*
>
> *…*
>
> *(7) The subject person shall make appropriate arrangements for the protection of clients' assets held under control and shall ensure that such assets are placed under adequate systems to safeguard such assets from damage, misappropriation or other loss and which permit the delivery of such assets only in accordance with the terms and conditions of the agreement entered into with the client.'*

The Arbiter is of the view that for the general fiduciary obligations to apply in the context of the VFA ACT, there must be something which is truly out of the ordinary and which should really act in a conspicuous manner as an out of norm transaction which triggers the application of such general fiduciary duties. No such out of norm event can be claimed during the short period of 3 weeks when the fraudulent transfers were happening.

The Arbiter thus considers that the Service Provider did not breach, in terms of the provisions outlined in this decision, the duty of care and fiduciary obligations towards its customer, the Complainant, when considering the particular circumstances of this case.

Decision

The Arbiter sympathises with the Complainant for the ordeal he suffered as a victim of a scam but, in the particular circumstances of this case, he cannot accept the Complainant's request for compensation for the reasons amply mentioned. The Arbiter is accordingly rejecting the Complaint.

However, since trading and investing in crypto assets is a new area in the financial services sector, the Arbiter would like to make a few observations.

Apart from the high risks and speculative nature commonly associated in trading with crypto, a consumer venturing in this area needs to be conscious and aware of the additional risks being taken, also, due to other factors including the risks associated with the infancy of the regulatory regime applicable, if at all, to this sector in general, which may not provide the same safeguards and protection normally expected and associated with other well-regulated sectors of the financial services sector.

Moreover, given the increasing and alarming volume of scams and fraud existing in the crypto field, retail consumers need to, more than ever, be vigilant and take appropriate and increased measures to safeguard themselves as much as possible to minimise and avoid the risk of falling victim for scams and fraud.

Retail unsophisticated investors would do well if before parting with their money they bear in mind the maxim that if an offer is too good to be true, then, in all probability, it is not true.

The Arbiter cannot help but notice the lack of or inadequate knowledge that many retail consumers have with respect to the various risks applicable to this area and on how to better protect themselves, despite the rush by many to join and participate into this sector.

The Arbiter considers that much more needs to be done on this front, apart from in other areas, to better protect consumers. Service providers operating in this field need to also do their part and actively work to improve their onboarding process by evaluating the much-needed knowledge of benefits and risks for consumers who opt to venture into this field.[54]

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

Alfred Mifsud
Arbiter for Financial Services

[54] It would not be amiss if at onboarding stage, retail customers are informed of typical fraud cases involving crypto asset transfers and warned against get-rich-quick schemes.

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 on expiration of the period for appeal. Personal details of the Complainant(s) will be anonymised in terms of article 11(1)(f) of the Act.