Before the Arbiter for Financial Services

Case ASF 162/2024

CL

('the Complainant')

vs

Foris DAX MT Limited (C 88392)

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

Sitting of 24 January 2025

The Arbiter,

Having seen **the Complaint** dated 21 August 2024[1] relating to the Service Provider's alleged failure to prevent, stop or reverse the payment in crypto of 60,277.27USDT[2] made by the Complainant himself from his account held with *Crypto.com* to external wallets allegedly owned by third parties who could be fraudsters or connected to fraudsters.

The purchase of these crypto assets was financed by a series of transfers in Euro from his account at Bank of Valletta collectively amounting to €65,444.57 spread over 30 transactions effected between 22 October 2022 and 15 May 2023.

This Complaint is a mirror image of a similar complaint raised by the same Complainant against Bank of Valletta related to the same transactions which transferred his funds from Bank of Valletta to his account with Crypto.com (operated by Foris DAX).

[1] P. 1 - 7 and attachments p. 8 - 11

[2] Tether (USDT) is a stable coin pegged at 1-to-1 with a matching fiat currency and backed 100% by Tether's reserves

Decisions on both complaints (against Foris DAX and Bank of Valletta) are being issued in parallel.

The Complaint

The Complainant opened an account with the Service Provider on 21 October 2022. Between 22 October 2022 and 09 May 2023, he carried about 30 transactions involving transfer of fiat currency amounting to about €65,500. On each of these occasions, the funds were immediately converted to USDT and transferred out to external wallets.

The Complainant stated that:

'***The complaint pertains to my Crypto.com account registered under the email .....@hotmail.com, which was active between October 2022 until mid-May 2023. During this period, the total amount of transactions performed amounted to EUR65,444.57, comprising approximately 30 transactions. I am a citizen of Malta and when I signed up, relationship with the platform is through the Malta regulated entity.***

During said time, I incurred significant losses through the mobile application platform of Foris DAX MT Limited, as it permitted unauthorised third parties to execute deceptive schemes, directly affecting me.

As a result of these actions, I suffered financial losses and was exposed to the systematic flaws within the operations of Foris DAX MT Limited. It is evident that Foris DAX MT Limited failed in its duty, and was negligent in performing adequate due diligence concerning my personal situation. The company failed to assess the risk tolerance before accepting funds, as demonstrated by the fact that my profile was only updated after the complaints had already been lodged. Accordingly, this indicates a disregard for the financial well-being of clients, and the suitability of investment opportunities being offered.

Moreover, even though the service provider does not fall under the PSD, that is, the Payment Service Directive, it still has similar obligations as a class 3 Virtual Financial Asset Provider, since its functions are similar. Indeed, its functions include the execution of orders on behalf of other persons dealing on own account, and carrying out both custodial or nominee services.

- ***Foris DAX MT Limited, the service provider, had failed to prevent or reverse the payments made in crypto assets from my account to a fraudulent third party.***
- ***I had believed that the trading platform through which I was sending my money, was legit and secure, but it turned out to be a scam.***
- ***Foris DAX MT Limited not only exposed my infrastructure to fraudsters but, also, failed to prevent the illicit transfer of wealth caused by the alleged fraud.***
- ***The Service Provider neglected to undertake adequate anti-money laundering and know your customer procedures, resulting in a number of fraudsters having access to the trading platform.***
- ***Foris DAX MT Limited failed to notice clear signals that the transfer effected by myself to the third party was suspicious and, therefore, had a duty to inform me of such, a warning which was never communicated.***
- ***The Service Provider also failed to have monitoring systems in place to distinguish between normal trading activities and those indicative of an illegal enterprise.***
- ***Finally, since Service Provider did conduct the necessary due diligence, I proclaim that the former had aided and abetted, albeit indirectly, the execution of fraudulent transactions causing me personal financial harm.'***[3]

Complainant basically raises these issues:

- Service Provider should have realised that external wallets to which his digital assets were being transferred were owned by fraudsters.
- Crypto.com should effectively communicate the potential risks associated with non-custodial wallets to their users and implement appropriate measures when they observe significant transactions being directed to non-custodial wallets from their platforms.

[3] P. 3

- Foris Dax should have been aware of the scams being carried out and were grossly negligent for not stopping such fraud.

Complainant accused Service Provider of misconduct and neglect and demanded full refund of his loss amounting to €65,444.57 citing as a reference Arbiter's decision in case ASF 116/2023 where Arbiter ordered a local bank to make full refund to a client who was defrauded.

Reply of Service Provider[4]

In their reply of 29 May 2024, Service Provider explained that Foris DAX MT offers the following services:

- ***'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 21 October 2022.***
- ***The Company notes that in the submitted complaint file, (the Complainant) has outlined his desired remedy as: (i)reimbursement for incurred financial losses.'***[5]

They gave a detailed sequenced of the various transactions executed by the Complainant on his wallet.[6]

They concluded that:

[4] P. 17 - 40 and attachments p. 41 - 91
[5] P. 17
[6] P. 18 - 39

'*In summary, (the Complainant) has withdrawn the total amount of 60,277.27 USDT from his Crypto.com Wallet towards external wallet addresses between March 9, 2024 – March 27, 2024.*

The wallet addresses in question are:

Oxdda1276ca92d62c4b7c84512100fab9dXX92cfea

Ox21D3641C6409890230c342887e1caXX7a03e7c96

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

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

As outlined above in the Foris DAX MT Limited Terms of Use, the Complainant is solely responsible for the security and authenticity of all instructions submitted through the Crypto.com App, and as such, the Company cannot accept liability for the veracity of any third party or for the instructions received from the Complainant themselves.'[7]

Hearings

During the first hearing held on 19 November 2024, the Complainant said:

'So, the account was opened before the 26th of October 2022. Basically, we started sending money there. I wasn't doing it alone because I didn't know how to do it. She, the scammer, was leading me how to do it.

I say that when I opened the account with Crypto.com, they asked me to show the ID card, to send a photo of my face and they asked me what my income is roughly. I do not remember exactly what amount I told them but it was a small

[7] P. 39 - 40

amount around €10,000 to €20,000 per year. There is a tick box and you choose it when you apply.

So, we started sending around €1,000 every time, or €1,500 or €2,000 from the period of 26 of October 2022 till the 15th of May 2023, in total around 31 transactions for approximately €65,000.

The reason for sending out this money was that she was telling me that I had to invest to get money back and when I put more money, I could earn more money faster. So, she was telling me to put more. I was telling her that there was no need because it was OK like that.

I say that from the bank, you send the money to Crypto and then, in Crypto, on the app, you can change the money to USDT and then, from there, you send them directly to your Fiat Wallet which is connected to the Crypto app.

And the scammer was taking the money from that Wallet, the Fiat Wallet. I was seeing that the numbers were changing, and I thought that the money was still there but when I tried to get them back, they were gone.

I say that during all this time with all these transactions, I did not know that I was being scammed. Otherwise, I would not have put them there.

I say that I have never traded in crypto before October 2022.

I say that nobody from Crypto.com ever spoke to me on how to trade.

When I got to know that I was being scammed, I tried many ways to contact Crypto or to contact someone, but they told me that they have no access to it and that they could not help me.

They did not try to recover my funds and make a chargeback to return my money. They did nothing.

I say that I was never aware that when I was sending money out to another Wallet, I was actually sending them to a third party. I was all the time thinking that I was sending them to myself.

I say that after I got scammed, the company did not contact me for due diligence. Nobody contacted me.

I say that I never disclosed my income to Foris DAX, like providing a tax return because they never asked for it.

They just ask you how much you earn roughly before you do the app. And then, you press the one that fits you according to your income. Then you continue filling up your details and address. I say that this was before.

I say that when I got to know that I was defrauded, I complained to Crypto.com but they did not change anything. They told me that once you do the transactions, there is no turning back. They told me that they could not get the money back from the blockchain. So, they told me that they could not help me.

I say that I never got any warning signs or any flag transactions from Crypto.'[8]

On being cross-examined, he said:

'I confirm that I opened my Crypto.com account and I performed all of the transactions within the account. But I say that I was not doing it alone. It was like I was forced to do it.

Asked whether I followed the instructions of this lady friend I was speaking to, I say, yes.

It is being said that from my transaction history, one can see that between the 27th of October 2022 and May the 9th of 2023, I made a number of withdrawals to two different external wallet addresses. Asked who gave me these external wallet addresses to make the withdrawals to, I say that it was the scammer.

It is being explained to me that external wallets are wallets that are not hosted by Crypto.com.

They are external wallets which either could be hosted by another exchange platform, or they could be DeFi wallets which are not hosted; they are unhosted wallets. But, in general, it just means they are not Crypto.com wallets.

I say that in my application, when I send the money to Crypto – let's say if I send €1,500, I would open the Crypto on my phone, on my application and when it arrives, I can see it there. And then, we will change it in the Crypto from Euro to USDT and then I had the DeFi Wallet connected with my Crypto.com application

[8] P. 94 - 95

and then I was sending them to this DeFi Wallet. It's like an external wallet connected with Crypto application.

It is being said that probably it was connected because before I withdrew anything to this Wallet, I would have had to add it to a whitelisting Wallet for my protection.

It is being said that if it was added to my list of whitelisted wallets, it would be in my list of pre-approved wallets.

It is being explained that before I can withdraw any crypto to a new Wallet that I have never withdrawn to, I need to add this Wallet to a list called Whitelist. I would need to input that number.

I say, yes, it was connected.

Asked to confirm whether these two Wallet addresses with the very long numbers and letters were provided to me by the scammer; that she told me to send the crypto to these Wallets, I say, yes.

Asked to confirm that throughout my use of the Crypto.com app and my account, Crypto.com fulfilled my instructions to purchase USDT and to make the transfers to Open Withdrawals to the two wallet addresses pursuant to my instructions, I say, yes.

Asked when I was given the Wallet address which had the long list of numbers, or when I was speaking to this person whether I asked questions to this person whether this Wallet number was fraudulent or not; and asked whether I made any enquiries myself on the specific address given, I say, yes, of course, I told her that I did not want to get defrauded. She was telling me, 'This is yours. This is your legitimate address. I don't have anything to do with it. Don't show it to me; I don't want to see it.' I asked because I was thinking that something may happen because I had never tried this before so, I was afraid of doing it.

Asked whether I asked the bank, I say that at first, I did not ask the bank, but when I sent the first amount, I told her to send it back so that I can check whether I can take them back or not.

And eventually she sent them back, and I got them back. So that's why I trusted.'[9]

[9] P. 96 - 97

During the second hearing on 26 November 2024, the Service Provider submitted:

'The case of the service provider that we can see from the records of the Complainant and his account was Crypto.com, that he carried out a series of transactions between October 2022 until May 2023. In these transactions, he withdrew cryptocurrency after purchasing them, generally through what we call the Fiat wallet. You would have purchased this through transfers from his bank account and subsequently sought to withdraw them. He ended up withdrawing them over these nine months to two different wallet addresses.

Now, in all instances of the transfers, the Complainant does not contend that he was the one who authorised these transactions and that was he himself, who authorised and chose the different wallets to withdraw.

I believe that in his evidence, he said that he was never aware to whom he was sending money to. He thought he was sending them to himself, but that actually demonstrates that it was the Complainant himself who authorised transactions, even if he was of his own mistaken belief. Now what we would say in these circumstances are that the terms and conditions of our Terms of Service make it very clear that The Complainant or the user is to be responsible for these transfers that they authorise themselves.

In our case, we are merely carrying out the instructions of the users and we carried them out faithfully. And, on that basis, we don't believe we are responsible for any sort of scam activity or any losses that he suffered. As you will know, all these transfers happen immediately. All the transactions are immutable and it's not for us to reverse them. And, in any case, we were only contacted with these complaints sometime after the last transaction occurred.

So, in our submission, we are not responsible for these transactions. We sympathise with the Complainant in that he may have been a scam victim. But as a matter of fact, he chose to make these withdrawals to these non-custodial accounts. These third-party accounts are not operated by Crypto.com and as such we are not responsible for any losses that he may have suffered. So those are our submissions.'[10]

[10] P. 100 - 101

On being cross-examined, he stated:

'I am being asked to confirm what due diligence we requested from the Complainant and what documents we have when The Complainant opened his account; whether we checked if he had any level of experience as a user of Crypto and what documents we collected.

I say that we collect all the necessary documents as is required per our licenses. And I think it's important at this point to understand that the license that we hold is different from the one that banks may hold. The licenses we hold are virtual asset service providers and, generally speaking, that requires us to carry out Know Your Customer information regarding the Complainant. At the account opening, this would require him to prove his identity, to submit documents which match his particulars; and for us to then conduct a visual identification of whether his selfie or his immediate live capture matches the photos provided on his identification materials. So, generally speaking, this would be some form of ID card or identification particulars to outline his personality, such as a birthday, his name and, finally, the live capture of his face upon making this account.

Being asked with regards to income whether hypothetically, if the Complainant wanted to invest €1,000,000, would we have accepted them and asked whether we have any caps, I say that our compliance obligations are not the subject of this trial and, in any case, it's not for us to reveal exactly what the compliance thresholds are.

We would say that in all circumstances our monitoring all transactions is live, we do check transactions which occur. None of the transactions which the Complainant carried out triggered any need for us to carry out such checks. And, as such, we are operating completely in accordance with our licenses.

I am being asked whether at the first time that the Complainant funded his account were there any caps, for example, up to €1,000 we do certain due diligence, from €1,000 to €20,000, we do another due diligence. Also, whether we request any information like banks do, I say that hypothetically, if the Complainant was to carry out a $1 million transaction, we would have checks on him. In the case of the Complainant himself, what he did was he carried out transactions which were relatively small accounts of around €1,000 to begin

with. He carried these out regularly. He carried these out with repeated occurrences over time; he even received an inbound transfer himself of cryptocurrency from Wallets which he sent to.

Asked whether when he opened the account, he should have marked a thick box of his earning, I say that I believe an indication is given, yes.

Being asked if his tick box was on the low side, how would we allow for the Complainant to put in money for five times as much of his declared income, I say that I am not sure if the Complainant has given any evidence as to what he ticked when he signed up for this account.

What we will say is that the transactions which he authorised are within the thresholds that we have to observe for the purposes of our license.

Asked whether we ever put a trigger on his incoming transactions, I say, if I am not mistaken, that his transactions were purchases of cryptocurrency, but he made these purchases through his VISA card or through transfers from his bank account. In the case of transfers through his bank account, they are monies that are already there and present such that he already owns them. In the case where they're triggered by cryptocurrency purchases through a VISA card or a credit card, they have to apply to his limit, which are authorised and also tested by the banks themselves. So, these purchases he made with us are within his means.

Asked whether we possess any documentation with regard to the Complainant's income, I say that I don't believe we do on this occasion, but I would have to check to be sure.

When we filed our evidence with the OAFS, we have included documents to show each and every purchase he made. These purchases show that the payment method across his different purchases over his history with us were generally made through debit card.

The Arbiter states that he has the full information that there were four payments which were made by bank transfer, the rest were made by debit card. And all originated from the same service provider. It was a bank to bank transfer all the way.

Mr Julian Yeung states:

What we're pointing out is that these are transfers of bank to bank. As you say, Mr. Arbiter, but more importantly through debit card, which means that the funds were already held in his account. So, the source of funds, as we can see here, came from his own holdings.

The Arbiter states that he understood that the point being made was that in the application for setting up his Crypto account, he ticked the box which gives a low 5-digit figure as annual income. But he has no evidence that this was supported by any documentation. It's just tick boxes.'[11]

Final Submissions

In their final submissions, the Service Provider basically repeated what was already covered in their reply and during the evidence at the hearings.

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

Further Considers:

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[12] which stipulates that he should deal with complaints in '*an economical and expeditious manner'.*

<u>The Service Provider</u>

Foris DAX is licensed by the Malta Financial Services Authority ('MFSA') as a VFA Service Provider as per the MFSA's Financial Services Register.[13] It holds 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').

[11] P. 101 - 103
[12] Art. 19(3)(d)
[13] https://www.mfsa.mt/financial-services-register/

As per the unofficial extract of its licence posted on the MFSA's website, the Class 3 VFAA Licence authorises Foris DAX 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.[14]

As outlined in the disclaimer section of the *Crypto.com* website, Foris DAX is *"trading under the name 'Crypto.com'" via the Crypto.com app'*. [15]

The Application

The *Crypto.com App* is a *'mobile application software developed, owned and released by Crypto.com and available for download for Android or Apple iOS …'.*

It offers the account holder *'a crypto custodial wallet'* and *'the purchase and sale of digital assets through the Wallet'*.[16]

Observations & Conclusion

Summary of main aspects

The Complainant made a transfer of his digital assets using the *Crypto.com* App. The said transfers were made to external wallet addresses thinking these belonged to him but evidently controlled by fraudsters who were leading him on with the false promise of quick profits. 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 beneficial owners are not known to the transferor. The Service Provider has no obligation under current regulatory regime to keep or make available information relating to external wallets.

In essence, the Complainant is seeking compensation from Foris DAX for the Service Provider's failure to prevent, stop or reverse the payments he made to the fraudster.

[14] https://www.mfsa.mt/financial-services-register/
[15] https://crypto.com/eea/about
[16] P. 17

The Complainant *inter alia* claimed that the services provided by Foris DAX 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.

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.

Applicable Regulatory Framework

As outlined above, Foris DAX is 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'*[17] 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[18] also issued Implementing Procedures on the Application of Anti-Money Laundering and Countering the Funding of Terrorism Obligations to the

[17] Guidance 1.1.2, Title 1, *'Scope and Application' of the 'Guidance on Technology Arrangements, ICT and Security Risk Management, and Outsourcing Arrangements'*.
[18] Malta's Financial Intelligence Analysis Unit being competent authority of AML issues

Virtual Financial Assets Sector.[19] 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 for the reimbursement by the Service Provider of the sum the Complainant himself transferred to external wallets 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 DAX, to allegedly fraudulent external wallets causing a loss to the Complainant of approximately €65,500.

  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. This is also given the nature of the transaction which involved crypto assets, the type of service provided, and other reasons as outlined below.

- The obligation for VFAs to identify the beneficial owners of unhosted wallets was not part of the regulatory regime at the time of events that gave rise to this complaint. VFAs obligations of due diligence relate to their own customers, in this case, the Complainant, not to owners of the unhosted wallets recipients of crypto assets transferred by their client.

[19] Layout 1 copy (fiaumalta.org)

Obligations for VFA's to identify such beneficiaries will only enter into force in 2025 in terms of **EU REGULATION 2023/1113 OF 31 May 2023 on information accompanying transfer of funds and certain crypto assets** as further explained in the **EBA Guidelines on information requirements in relation to transfers of funds and certain crypto-assets transfer under Regulation EU 2023/1113 (Travel Rule Guidelines – reference EBA/GL/2024/11 of 04/07/2024.)**[20]

- 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 *'external wallets'* owned by the Complainant and hence the Service Provider had no information about the third party to whom the Complainant was actually transferring his crypto assets.

  Furthermore, the Complainant must have himself 'whitelisted' the address giving all clear signal for the transfer to be executed**.** 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 Complainant contacted the Service Provider after all alleged fraudulent transactions were executed.

  Once finalised, the crypto cannot be transferred or reversed as specified in the Service Provider's Terms and Conditions of Use (and as typically indicated on various other internet sites).[21]

  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 DAX.

[20] In particular article 4.8, para. 76 - 90

[21] E.G. https://www.chargebackgurus.com/blog/chargebacks-more-volatile-complex-than-cryptocurrency

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 …'.[22]

It is also noted that Clause 7.2(d) of the said Terms and Conditions which deals with *'Digital Asset Transfers'* further warns a customer about the following:

'We have no control over, or liability for, the delivery, quality, safety, legality or any other aspect of any goods or services that you may purchase or sell to or from a third party. We are not responsible for ensuring that a third-party buyer or seller you transact with will complete the transaction or is authorised to do so. If you experience a problem with any goods or services purchased from, or sold to, a third party using Digital Assets transferred from your Digital Asset Wallet, or if you have a dispute with such third party, you should resolve the dispute directly with that third party'.

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

The current regulatory regime applicable to a VFA Service Provider is different from and does not reflect the requirements and consumer protection measures applicable to banks and financial institution falling under EU regulatory regimes.[23]

[22] P. 40

[23] Financial institutions based in Malta are regulated under a separate and distinct regulatory framework, namely, that provided for under the Financial Institutions Act (Cap. 376) which also covers the Payment Services Directive (PSD2), (Directive EU 2015/2366 on payment services in the internal market).

It is probable that as he himself admitted the Complainant has unfortunately fallen victim of a scam done by a third party and no evidence resulted that this third party in any way related to the Service Provider.

- Ultimately, the Arbiter does not consider that in the case in question, there is any clear and satisfactory evidence that has been brought forward, and/or emerged, during the proceedings of the case which could adequately corroborate that the Service Provider failed in any of the applicable obligations, contractually and/or arising from the VFA regulatory regime applicable in respect of its business.

- The Arbiter notes that the crypto business is a relatively new area with no *harmonised regulation* existing at the time of the disputed transactions. A regulatory framework is still yet to be implemented for the first time in this field within the EU.[24]

  Whilst this area of business remains unregulated in certain jurisdictions, other jurisdictions, like Malta, chose to regulate this field in the meantime and subject it to a home-grown national regulatory regime. While such regimes offer a certain amount of security to the consumer, since they are still relatively in their infancy, may not necessarily reflect the same standards and protections applicable in other sectors of the financial services industry which have long been regulated.

  A person who chooses to venture into the area of crypto which, itself, is typically a highly speculative and risky market, needs to also be highly conscious of the potential lack of, or lesser, consumer protection measures applicable to this area of business, as compared to those found and expected in other established sectors of the financial services industry. EU regulatory bodies have issued various warnings to this effect over the past years.[25]

[24] Provisional agreement has been reached on the EU's Markets in Crypto-Assets Regulation (MiCA) only in June 2022 - https://www.consilium.europa.eu/en/press/press-releases/2022/06/30/digital-finance-agreement-reached-on-european-crypto-assets-regulation-mica/
MiCA is expected to enter into force in 2025 – https://www.financemagnates.com/cryptocurrency/can-mica-take-europe-to-the-crypto-promised-land/

[25] https://www.eiopa.europa.eu/document-library/other-documents/crypto-assets-esas-remind-consumers-about-risks_en

The Arbiter notes that the Complainant makes a strong argument that the Service Provider has failed its AML obligations and, consequently, it has not triggered dutiful warnings to the Complainant to alert him to the possibility of his being scammed.

The Arbiter has no competence to investigate AML failures and any such claims should be directed to the competent authority in Malta, the FIAU, who have the competence and expertise to investigate such claims.

The Arbiter, however, notes that in other cases before him, strong assertions were made by the Service Provider that they adhere to all AML obligations, including the monitoring obligations imposed by Section 2.3 of the Implementing Procedures earlier referred to in this decision.

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**

https://www.esma.europa.eu/sites/default/files/library/esa_2022_15_joint_esas_warning_on_crypto-assets.pdf

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.[26]

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.

[26] 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.

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.
