Before the Arbiter for Financial Services

Case ASF 107/2024

FL

(the 'Complainant')

vs

Foris DAX MT Limited

(C-88392)

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

Sitting of 7 March 2025

The Arbiter

Having considered in its entirety, the Complaint filed on 21 May 2024, including the attachments filed by the Complainant,[1]

The Complaint

Where, in summary, the Complainant claimed that he opened an account with the platform 'CRYPTO.COM' and deposited funds from his external bank accounts to fund the former account, in order to be able to acquire digital assets, such as cryptocurrencies.

However, from September 2022 to June 2023, the Complainant fell victim to a romance scam. In September 2022, he met a person on Facebook who presented herself as 'Julia Smith'. The two communicated until June 2023.

At first, the relationship appeared ordinary and personal in order to gain the Complainant's trust, as Mrs Smith led him to believe in a romantic relationship

[1] Complaint Form from page (p.) 1 - 6, and attachments from p. 7 - 142

by "*intimately engaging with him, promising to meet in person, and indicating a desire to start a family life*".

However, the relationship quickly evolved into exchanges which primarily concerned financial investments. Mrs Smith presented herself as an expert in financial investments, using the performances of a broker, 'RARIBLE', whom she claimed was serious. Hence, Mrs Smith had both an emotional and intellectual control over the Complainant.

The Complainant was eager to diversify his sources of investments and income, and Mrs Smith quickly took advantage of his ignorance and encouraged him to invest increasingly large sums of money on the platform in question to generate significant profits through trading and investment plans. In order to do this, the Complainant made transfers from his various bank accounts to various cryptocurrency platforms, including 'CRYPTO.COM', to finally fund his balance on the fraudulent platform 'RARIBLE', whose payment method was cryptocurrency.

The Complainant made payments amounting to €359,695 to cryptocurrency platforms in order to transfer them to 'RARIBLE'.

The Complainant lists the total amount of operations, converted into euros:

- €24,507.15 for withdrawals from 'RARIBLE' to 'CRYPTO.COM'
- €359,695.27 for the sums injected from 'CRYPTO.COM' to 'RARIBLE'
- Including €220 in commissions (€10 per transaction).

The Complainant claims that he lost €315,658.15 via the platform 'CRYPTO.COM'.

In March 2023, the Complainant decided to withdraw $110,200 from 'RARIBLE' after having invested substantial amounts of money and seen the significant gains displayed to him by the platform. This request was denied because to retrieve his funds, the Complainant was required to complete a 'capital verification procedure' which required him to deposit the same amount on the platform. The $110,200 for verification had to be returned with the $110,200 initially requested, totalling $220,400.

Once this verification procedure was completed with the help of Mrs Smith, who supposedly contributed around $29,000, the Complainant's request for the $220,400 was refused on the grounds that the funds came from two different accounts. Thus, he was asked once again to deposit $110,200 on the platform. On the insistent advice of Mrs Smith, who promised to help by depositing $25,000 directly to his 'UPHOLD' account, the Complainant took several loans to make the requested deposit.

In total, and following the threats made against him, the Complainant made ten payments totalling €330,787 before he realised that RARIBLE and Mrs. Smith were a fraudulent financial scam.

The Complainant alleges that 'CRYPTO.COM' bears some responsibility because the funds were able to freely pass through the 'CRYPTO' platform to the scammer's account without any warning to the Complainant about the exact nature of the 'RARIBLE' account.

Moreover, on 11 May 2023, 'CRYPTO' informed the Complainant that he would no longer be able to use his account without any explanation.

Consequently, the Complainant is asking the Service Provider to refund the funds illegaly taken by the scammer from his account, totalling €315,658.15.

The reply of the Service Provider[2]

***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.*
- *At the material time, Foris DAX MT Limited additionally offered a single-purpose wallet (the "Fiat Wallet"), which allowed customers to top up and withdraw fiat currencies from and to their personal bank account(s) for*

[2] P. 148 - 174 with attached documents p. 175 - 208.

the purposes of investing in crypto assets. Following a successful service migration on January 25, 2023, the Fiat Wallet service was migrated to Foris MT, a sister company of Foris DAX MT based in Malta.

- *(the "Complainant"), e-mail address xxxxx@orange.fr, became a customer of Foris DAX MT Limited through the Crypto.com App and was approved to use the Wallet on the 31 of October 2022.*
- *The Company notes that in the submitted complaints file, [the Complainant's] representative has outlined his desired remedy as: (i) reimbursement for incurred financial losses.*

They gave a detailed timeline of the transfers that were made from his Crypto.com account to four different external wallets.These were executed between 24 November 2022 and 05 May 2023 through 16 withdrawal transactions, collectively involving 320,252.48 USDT[3] and 22.881 ETH.[4]

The transferred crypto assets were funded by transfers in Euro currency as shown in the following Table:

DATE	EURO	TRANSFER FROM
16.11.2022	1013	Google Pay
22.11.2022	1006	Google Pay
30.11.2022	2000	BANK TRANSFER
01.12.2022	350	''
02.12.2022	28000	''
02.12.2022	1000	''
23.12.2022	6000	''

[3] USDT is the symbol for Tether, a cryptocurrency that is pegged to the U.S. dollar.
[4] ETH stands for "Ether" crypto token used by the Ethereum network.

06.01.2023	102000	‘’
26.01.2023	150	‘’
10.02.2023	2000	‘’
22.02.2023	100	‘’
28.02.2023	1500	‘’
01.03.2023	2000	‘’
02.03.2023	1500	‘’
03.03.2023	51000	‘’
03.03.2023	2000	‘’
04.03.2023	1790	‘’
07.03.2023	2000	‘’
10.03.2023	20	‘’
14.03.2023	550	‘’
21.03.2023	53999	‘’
22.03.2023	2000	‘’
23.03.2023	2000	‘’
24.03.2023	21000	‘’
25.03.2023	22650	‘’
05.05.2023	41500	‘’
TOTAL	Euro 349128	

The Service Provider stated that based on their investigation, they are unable to honour the Complainant’s refund request based on the fact that the reported transfers were made by Complainant himself.

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

They continued stating:

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

(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.

Whilst we fully empathize with (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 has no access to.

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."

Hearings

During the first hearing held on 8 October 2024, the Complainant submitted the following:

"***I have been using the services of Crypto.com between November 22 up to May 23, and I have been using this platform to transfer money to a platform called Rarible EX for the total of over €320,000 which I have sent through Crypto.com.***

My concern is the following. The platform Rarible EX is a scammer. My complaint is that Crypto.com should have checked this platform and avoided any transfers as the majority of major companies and banks do.

Actually, the use of Cypto.com has been advised by the scammer or the crook I was in touch with and now I understand why: because Crypto.com let the transfer go, they never check the honesty of Rarible EX like different major platforms do.

And, so, I have been transferring all that money without any control from Crypto.com; without any warning.

This is what my complaint is about: not checking the honesty of the platform Rarible EX. In fact, it is like letting them do what they want like scamming people."

The Arbiter pointed out that from the details of this case, it appears a total of about €350,000 were transferred and some of these funds were received back in the initial stages as a teaser (a manoeuvre of the fraudster to build up trust). So, in total, the claimed loss amounts to €315,658.

"I say that this is correct.

The Arbiter understands that these payments were made to my account with Crypto.com by transfers of Euros from my banks N26, Boursorama and BNP Paribas.

Asked by the Arbiter whether I made any claims in France against my banks for neglecting to warn me not to transfer these funds to my Crypto.com account, I say that the point is not the matter of the transfer from my banks to Crypto. The matter is the transfer from Crypto to Rarible EX because Rarible EX is a scammer and there was no security.

As to claims against my French banks, I say not yet because there was only one transfer from BNP and then they blocked everything.

As to the other banks, Boursorama and N26, so far no, because like I said, Crypto.com is supposed to be a major platform and, therefore, they should ensure the safety and security of the customers. The matter is Crypto itself."[5]

During the second and final hearing held on 19 November 2024, the Arbiter waived contumacy rules for the late reply of the Service Provider and invited them to cross-examine the Complainant in relation to his evidence at the first hearing.[6]

The Complainant answered:

"***It is said that in my letter of claim, I say that the reason why I wanted to have an account with Crypto.com was so that I could freely and simply acquire digital assets such as cryptocurrencies. Asked whether it is correct to state that it was of my own volition that it was I who actually wanted to trade in digital assets, I say, yes.***

It is being said that it seems that according to the statement on Page 8 of my complaint, my earliest investment or payment to Rarible was around November 2022. And that there were a number of subsequent transactions ending in 2023.

Asked when I realised after the first or second transaction that there was no profit received or there was nothing executed as was promised by the fraudster

[5] P. 210 - 211
[6] P. 220 - 223

why did I want to continue investing my money, hoping for a profit, or when none was received with the first few transactions, I say because basically they are scammers and they were asking for a kind of security deposit.

And my point is that the very basis of my complaint is that Crypto.com is supposed to be a major cryptocurrency platform. They should have been aware of the scammers dealing with cryptos and all that thing. I say that my basic point is that I never got a message from Crypto.com warning me to pay attention because the site that I was using, Rarible EX is a scammer.

It is being said that I continued transacting from 2022, and there are a number of transactions that I made, and I was led to believe that as soon as I placed that money my Crypto account, I would receive a kind of profit or that I would make more money when that was never received.

Asked why I continued investing in crypto, I say because they were saying that there was a level of investment to get to that but then, I realised through different messages that, in fact, it was a scam.

Asked what steps I took to make sure that the wallet address that I was sending the funds to was legitimate, I say that at the very beginning, I made some investments and I got some profit as a kind of 'assurance' to the beginner or the one who is being scammed. So, I continued to invest. The point is that I do not understand how a platform like Crypto is not aware of all these scammers around because from other different platforms, I got the message that I was not able to make transactions. I do not understand why.

I am being asked again what steps I took to make sure that the address that I was instructing Crypto to remit my funds to was legitimate.

I reply by saying that I made an investment at the beginning and then I received a 30,000 something, the equivalent of €40,000. So, at the beginning it was working properly and then, let's say, for security reasons from them or safety or whatever, I was asked to put some more money. And then, I realised that it was a scam and that I will never get any profit or my money.

I say that I checked on Google and on other different sites, for information about Crypto and on all the other platforms whether it was a scam or whether

it was a safe one. And I never succeeded to get information about that. Otherwise, I should have stopped long before.

Asked whether I asked my bank to verify whether the wallet address given to me was a legitimate one, I say, no, because banks in France, by principle, do not want to hear about cryptocurrencies.

Asked whether it is correct to say that Crypto actually executed the instructions given to them by me, so what Crypto did was transfer the funds to the address that I indicated to them each and every time, I say, yes.

Once again, I say that I think that a platform like Crypto should be aware of – and I am sure that they know – of all the scamming sites but they don't inform their customers. That's my point.

I am being referred to my statement where I mentioned that other crypto platforms stopped me from carrying out my transactions, and asked whether that is right, I say because, in fact, we have some other platforms, but I have never been able to open an account. I do not know why. I started an account with Crypto but I have never been able to start with others.

Asked whether it is correct to say that someone gave me some warnings about my transactions, I say, yes, for example, Binance. In fact, Binance did not proceed with the transfer; it was not a warning, they did not proceed with the transfer.

The Arbiter asks me whether they stopped me from having an account or whether I had an account and they stopped me from making the transfer.

I say that I have an account with Binance, but when I asked for the transfer, it has never been processed. I did not get any information why it has not been processed, but it has not been processed at all.

I say that I had sent money to my account with Binance. I had money in my account and I had digital assets in my account and I asked for those digital assets to be transferred and, then, since it was not working, I brought my money back.

And that's my point about security and so, the scammer or the crook I was in touch with said, 'OK, so you have troubles with that platform. You should use

Crypto instead.' Crypto platform has been advised by the scammer or by the crook and that's my concern. In fact, there is a major concern about, let's say letting the transfers and not checking because, Crypto, as a major platform, I'm sure that they have many more tools to check whether a site where the money is transferred is a scam or a crook. Do you see what I mean?

Asked in the circumstance where a platform didn't allow me to carry out my transaction whether I then carried out the transaction on another platform such as Crypto.com, and asked when I received these warnings, whether it was during the period of November 2022 to May 2023, I say, Binance, I never got a warning. In fact, it was the same period; it was just before starting with Crypto, because, in fact, basically, since it didn't work with Binance, then the crook advised me, 'Oh! go with Crypto it will work easily.'

Asked whether it is fair to say that after I received the warning from Binance, I carried out the same transactions I was warned about on Crypto.com, I say, once again, I did not get any warning from Binance.

They did not process the transfer without any warning or without any explanation, so I didn't know why it was not working. But, of course, if I had received a warning from Binance saying, 'Oh! Take care! This is a scam,' or 'This is unsafe,' I will never have processed from any other platform including Foris DAX.

It is being said that actually then part of my earlier testimony was incorrect, that I never received a warning from anyone.

I say, no.

It is being said that either I received the warning and I proceeded to carry out the transactions on Crypto.com, or I never received a warning at all. So, asked which one is it, I say that the transfer has not been processed but it was not a warning about Rarible EX.

So, it is being said that in that case, I never received a warning. Other platforms didn't carry out my transaction, but I never received a warning. Asked whether this is correct, I say, yes.

It is being said that I never received a warning from another platform, and I have instances where other platforms do not carry out my transaction.

I say they just did not proceed with my transfer.

I receive a warning about cryptocurrency, generally speaking from my French banks. That's it.

So, it's being said that I received a warning from my banks about cryptocurrency and I did not receive any warning from another platform about the transaction, I say, globally speaking, even when I try to transfer my money from French banks to Binance, then, in fact, I went through another, China.

It is being said that what I am saying is that despite receiving warnings about cryptocurrency, I proceeded to invest in them anyway.

I say, yes, because I have a friend in France who invests in cryptocurrencies, but unfortunately, instead of investing in cryptocurrency on Crypto, for example, and buying cryptos by Crypto.com or other platform, I went to another, let's say, crook, Rarible EX, and that's the point."[7]

Mr Julian Yeung, on behalf of the Service Provider, submitted:

"***Our summary of the case is that between the dates of November 24, 2022, to May 5, 2023, the complainant carried out a series of transactions whereby he purchased cryptocurrency and withdrew the same to external accounts.***

We would state for the record that these accounts are not managed by Crypto.com and, as such, we don't know who these external wallets belong to. We don't carry out verification of these accounts because we're not obliged to by the law. The law only requires that we carry out verification and Know Your Customer obligations for customers who register for an account with us.

With that in mind, we don't have proof of who these monies went to or who these cryptocurrencies were transferred to. All we can say, Mr. Arbiter, is that these transactions were carried out under the full authority of the complainant. It was the complainant himself who entered these external

[7] P. 220 - 223

addresses. From his testimony, it is the complainant himself who verified and processed these transactions. Therefore, we will say that these transactions were carried out solely and strictly in accordance with his instructions.

It is not for Crypto.com to verify where these addresses belong to or who these addresses go to, precisely because we have no legal obligation to do so. So, insofar that the complainant is concerned or makes a complaint that he was not warned for these transactions, we would remind him that there's no legal obligation to do so and, in fact, the warnings in the terms and conditions make it very clear that he should be responsible for the transactions that he himself authorises or the transactions are authorised on this account.

So, accordingly, and in conclusion, we continue to reject the allegation that we have any knowledge of these external wallets or who they belong to. There is no proof advanced by the claimant regarding the same and we will say that we carried out these transactions in accordance with his instructions and we did so legally."[8]

The Arbiter requested the Complainant to produce evidence of his request to another platform to make the transfers to the same wallet numbers in question where the other platform did not carry out the transaction. Such evidence as provided in pages 228 – 229 is not considered sufficient to prove why some transfers through Binance succeeded and others failed and that Binance refused to make transfers to the external wallets involved in this scam.[9]

The Arbiter requested from Foris DAX to produce a total declaration that at the time that the transfers were being made to the four wallets in question, they had no knowledge that there was any fraud history linked to any of these four wallets.

This declaration was duly sent and properly records the Service Provider's assertion that at the time the transfers were being executed, they had no alerts or warnings that any of the external wallets had a history or were linked to fraud.[10]

[8] P. 224

[9] See also p. 307 points 12 to 15 which explain in detail why Complainant did not provide evidence requested that Binance refused to make payments which Cryto.com allowed.

[10] P. 299 - 300

The Arbiter requested the Service Provider to submit KYC documents they obtained from Complainant at the onboarding stage. These were submitted.[11]

Addressing the Complainant, the Arbiter made reference to the transfers made by the Complainant from his three banks in France to Crypto.com, which banks have certain obligations of transaction monitoring in the European Union. The Arbiter remarks that these banks have a longer relationship with the Complainant than Foris DAX, as the latter relationship lasted only a few months whereas normal relationships with banks last much longer.

Thus, the Arbiter asked the Complainant whether he has made his case to the three banks, to which the Complainant replied:

"***I have two French banks and, in fact, they did not allow any transfer to Crypto or to Binance telling me that they are not processing transfers to Crypto and to cryptocurrencies platforms. And the last one that I have been using, in fact, at the beginning a German bank and now it became a French bank. It's N 26.***

The Arbiter states that N 26 made the transfers for me. I say, yes, they made the transfers to Crypto.

Asked by the Arbiter whether I made my case against those two banks, I say, not yet."[12]

Decree

On 2 December 2024, the Arbiter issued a Decree *inter alia*, stating:

> "***The Arbiter requires a convincing explanation from Complainant as to whether or not he made a Complaint against his remitting banks (Boursorama, N26 and any other bank involved in the remittance of funds to his Crypto account) holding them responsible for not warning him about the possibility of such transfers being related to fraud. If such a complaint was made, the Arbiter requires copy of related exchanges translated to English.***
>
> ***It must be borne in mind that the transaction monitoring obligations envisaged in banking regulations primarily apply to banks. CASP***

[11] P. 233 - 238
[12] P. 226

> ***licensees like Foris DAX only have generic fiduciary obligations towards their clients but not the same transaction monitoring obligations applicable to Banks.***
>
> ***Without such evidence, the Arbiter is hesitant to make a final decision of this case which could create exposure to unjustified enrichment if the Complainant has made or will make claims for the same loss to banks that owe him much more forceful fiduciary duties under banking regulation for payments commonly referred to as PSD 2.***"[13]

The Complainant replied on 9 December 2024 stating:

> ***"I confirm that I never made a complaint against Boursorama and N26 banks and do not plan to do so in the near future."***[14]

Final submissions

The Complainant did not make any final submissions even though he was invited to explain further why he did not lodge a complaint against the French Banks.

The Service Provider was invited to address these points in the final submissions:

> "***The Service Provider's defence is basically that the transactions were undeniably authorised by the Complainant and that they were simply executing his instructions without having any alerts that the transferee wallets were controlled by fraudsters.***
>
> ***Yet, there could be a case to be answered (given that the relationship lasted more than 5 months during which a multitude of transactions were affected) about their general fiduciary obligations to their client. Under such obligations, a good conversation with the client should have been made about his experience in crypto trading especially when substantial payments started flowing through the account, in particular,***

[13] P. 232
[14] P. 242

transactions of €102K in January 2023, €51,000 and €48,000 in March 2023, and €41,000 in May 2023."[15]

In their final submissions, the Service Provider merely repeated the arguments made in their defence according to the reply and their evidence during the hearings.

Analysis and Considerations

Summary of main aspects

The Complainant made a transfer of his digital assets (USDT and ETH) using the *Crypto.com* app. The said transfers were made to four different external wallet addresses allegedly used by fraudsters. The transfers 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 regulatory regime existing at the time the transfers were made, to keep or seek 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.

The Complainant *inter alia* claimed that the services provided by Foris DAX were not correct given that it transferred the funds 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 a crypto withdrawal once the transaction was done on the blockchain.

[15] P. 302 - 303

Applicable Regulatory Framework

As outlined above, Foris DAX was at the time holder of a Class 3 VFAA licence granted by the Malta Financial Services Authority ('MFSA') under the Virtual Financial Assets Act, 2018 ('VFAA').[16]

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 was 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 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

[16] On 27 January 2025, the licence was surrendered and replaced by a new licence for Crypto-asset Service Providers under the MiCA regime as explained in footnote 25 https://www.mfsa.mt/financial-services-register/
[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.
[19] https://fiaumalta.org/app/uploads/2023/06/20210520_Revised-Implementing-Procedures.pdf

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 €316,000.

  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 should 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.

  At the time the disputed transactions took place, there was no obligation on the Service Provider to seek evidence on the identity of the beneficial owners of external (unhosted) digital wallets. These obligations are only now being gradually introduced effective 30 December 2024.[20]

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

[20] https://www.eba.europa.eu/sites/default/files/2024-07/6de6e9b9-0ed9-49cd-985d-c0834b5b4356/Travel%20Rule%20Guidelines.pdf particular reference to article 4.8.2, pages 30 -32

right part 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.

  Furthermore, the Complainant must have himself 'whitelisted' the address[21] giving an 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 address he himself provided.

- The Complainant seems to have only 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).[22]

  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.

  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

[21] P. 99

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

Instructions for a Digital Asset Transfer to Crypto.com as the Digital Asset Transfer may not be cancelled or reversed once processed …'.[23]

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 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.[24]

Indeed, if the Complainant is seeking protection similar to that offered in the EU under PSD 2 obligations applicable to banks and payment institutions, he could seek advice on the appropriateness of seeking such protection from the bank(s) that made the fiat currency transfers to his Crypto account.

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 is 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 has just been implemented for the first time in this

[23] P. 174

[24] 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).

field within the EU but was not applicable at the time when the disputed transfers were made.[25]

Whilst this area of business had remained 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 offered a certain amount of security to the consumer, since they are still relatively in their infancy, they did 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.[26]

Final considerations

The Arbiter has also considered whether the Service Provider has failed to give customer the general level of protection provided in the VFA ACT (Chapter 590) Article 27 which 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

[25] 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 entered into force in 2025 – https://www.financemagnates.com/cryptocurrency/can-mica-take-europe-to-the-crypto-promised-land/

[26] https://www.eiopa.europa.eu/document-library/other-documents/crypto-assets-esas-remind-consumers-about-risks_en
https://www.esma.europa.eu/sites/default/files/library/esa_2022_15_joint_esas_warning_on_crypto-assets.pdf

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 Chapter 16), in so far as applicable."

In this context, Guidance Notes on this subject were recently published by the Arbiter which in respect of VFA licensees, state 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[27] 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),[28] 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.[29]

***Compliance with such recommendations or lack thereof will be taken into consideration in future complaint adjudications**."*

[27] *Guidelines on information requirements in relation to transfers of funds and certain crypto-assets transfers under Regulation (EU) 2023/1113* - EBA/GL/2024/11 of 04/07/2024
https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32023R1113
https://www.eba.europa.eu/publications-and-media/press-releases/eba-issues-travel-rule-guidance-tackle-money-laundering-and-terrorist-financing-transfers-funds-and

[28] Such as Case ASF 158/2021

[29] Such as Case ASF 069/2024

The Arbiter cannot apply these Guidance Notes retroactively. Furthermore, the transactions history on the account with Service Provider placed the largest transaction very early in the relationship and subsequent transactions were possibly considered normal in the light of such a large previous transaction.[30]

The Service Provider maintain that any general fiduciary duty under the civil code is by virtue of Article 27 of the VFA ACT conditioned by the ***"in so far as applicable"*** term under 27(2). They argue that once the VFA ACT does not specifically impose on them transaction monitoring obligations other than for the purpose of AML/FT, no such fiduciary duties as provided by the civil code would apply. [31]

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.

In the context of the history of the transactions on this account, the only instance which could have given rise to such obligation is the transfer of €102,000 affected on the 6 January 2023.

However, this happened rather early in the relationship as shown in the Table below and the account had not yet built a pattern which would have made this payment a clear outlier.

DATE	**EURO**	**TRANSFER FROM**
16.11.2022	1013	Google Pay
22.11.2022	1006	Google Pay
30.11.2022	2000	BANK TRANSFER
01.12.2022	350	''

[30] Transfer of Euro 102,000 on 06.01.2023 when there was less than 7 weeks' transaction history on record.
[31] Case ASF 119/2023 as in defence of the appeal ref. 23/2024

02.12.2022	28000	‘’
02.12.2022	1000	‘’
23.12.2022	6000	‘’
06.01.2023	102000	‘’

Subsequent payments were then for smaller amounts as shown in the Table below:

DATE	**EURO**	**TRANSFER FROM**
26.01.2023	150	‘’
10.02.2023	2000	‘’
22.02.2023	100	‘’
28.02.2023	1500	‘’
01.03.2023	2000	‘’
02.03.2023	1500	‘’
03.03.2023	51000	‘’
03.03.2023	2000	‘’
04.03.2023	1790	‘’
07.03.2023	2000	‘’
10.03.2023	20	‘’
14.03.2023	550	‘’
21.03.2023	53999	‘’
22.03.2023	2000	‘’

23.03.2023	2000	‘’
24.03.2023	21000	‘’
25.03.2023	22650	‘’
05.05.2023	41500	‘’

They do not give rise to strong suspicion of fraud to trigger the general fiduciary duty as envisaged in the VFA ACT, conditioned as they are by the large payment of 6 January 2023 which made subsequent smaller payments look normal.

Finally, the Arbiter finds the Complainant’s reluctance to lodge complaints against his home banks who transferred funds to his crypto account, not only very strange, but suspicious given that:

1. He is seeking from a CASP the protection that should be primarily provided by his banks.

2. It could lead to unjust enrichment if such complaint against his banks is lodged after compensation is awarded by the Arbiter.

3. It may indicate that Complainant was in fact given due warnings by his banks (with whom he must have a much longer relationship) about the risks of investing in crypto.

In fact, during the hearing, Complainant admitted:

“I receive a warning about cryptocurrency, generally speaking from my French banks. That's it.”[32]

Furthermore, the Arbiter notes inconsistencies in the evidence of the Complainant. During the hearing, he said:

“I started an account with Crypto but I have never been able to start with others.”[33]

[32] P. 223
[33] P. 222

A few moments later, he said he had an account with Binance who refused to execute the transfers which Crypto.com found no objection to. Asked to produce evidence, no such evidence was provided.

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.[34]

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.

[34] 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.

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.
