Before the Arbiter for Financial Services

Case ASF 119/2023

LD

('the Complainant')

vs

Foris DAX MT Limited (C 88392)

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

Sitting of 22 March 2024

The Arbiter,

Having seen **the Complaint** dated 22 August 2023[1] relating to the Service Provider's alleged failure to prevent, stop or reverse the payment in crypto with a value equivalent to US$[2] 205,000[3] made by the Complainant himself from his account held with *Crypto.com* to three external wallets 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 17 November 2022. Between 17 November 2022 and 20 December 2022, he carried out 25 transactions involving transfer of fiat currency from his bank account in Israel in local currency. The fiat currency was converted in USDT[4] stable coins and these were regularly transferred to three external wallets so that in all Complainant

[1] P. 1 - 7 and attachments p. 8 - 94
[2] United States Dollars
[3] P. 4
[4] Tether (USDT) is a stable coin pegged at 1-to-1 with a matching fiat currency and backed 100% by Tether's reserves.

transferred USDT 200,795.02 to such wallets. The counter value in US$ today is about USD 200,000.

Complainant basically raises these issues:

- Service Provider should have realised that Complainant was inexperienced, and the frequency and size of the transfers should have alerted the Service Provider to detect the possibility of the Complainant being defrauded and should have intervened to alert him to such possibility.
- Complainant had been in regular contact with the customer service team of the Service Provider at the point of making the transfers and they never alerted him to anything not being in order.
- Service Provider failed to co-operate with the Complainant and with the Israeli Authorities, that were investigating the fraud, and failed to provide information which could have identified the fraudsters and help in recovery of the stolen funds.
- Service Provider has failed to meet its obligations under Anti Money Laundering and Finance of Terrorism regulations and such failure prevented early detection of the fraud which would have minimized the loss.

By way of compensation, Complainant was seeking around US$100,000.[5] The figure was arrived at by taking into consideration transactions exceeding the threshold of €15,000[6] as well as other transactions which, by virtue of their high value, should have triggered due diligence alerts within Crypto.com operational protocol.[7]

Complainant argued that following the first transaction exceeding €15,000, there were other transactions involving €148,423 which could have been avoided if he had been informed and educated regarding the potential risks or unusual nature of these transactions.[8]

[5] P. 4 - later revised specifically to US$103.079 (P. 220)
[6] The threshold of €15,000 is based on the definition of 'occasional transaction' in 2 (1) of Subsidiary Legislation 373.01 Prevention of Money Laundering and Funding of Terrorism Regulations.
[7] P. 220
[8] P. 217

The Complainant presented a professional report[9] he commissioned to T&H Consulting based in Hungary with a view to map the web of transactions of the funds he had transferred to the three external wallets and how these assets were moved subsequently.

This report identifies the scammers as '**Antrush Group Limited'** with website **aglvip.com**. It confirms that the USDT were transferred over 25 transactions to three external wallets. Subsequently, these funds were moved to other wallets as mapped in folio no. 89. There were 5 transactions involving payments of a cumulative, relatively small amount of USDT 2247.65 with the largest being USDT 1,139.43 and the smallest USDT 100. These were transactions effected between 21 November 2022 and 22 December 2022 and were made to wallets hosted by Crypto.com. Service Provider would have due diligence documents related to the owners of these accounts. [10]

Reply of Service Provider

In their reply of 15 September 2023, 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"), the purchase and sale of digital assets on own account, and 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) for the purpose of investing in crypto assets. Services are offered through the Crypto.com App (the "App"). The Wallet is only accessible through the App, and the later is only accessible via a mobile device.'[11]

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

They concluded that:

'*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*

[9] P. 69 - 90
[10] P. 78
[11] P. 100
[12] P. 101 - 123

transfers were made by Mr LD himself, and the Company was merely adhering to the Complainant's instructions and providing the technical service of transferring the requested assets to the address provided by him.

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 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.

Mr LD 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 accepted by the Complainant 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 Mr LD in this regard, it cannot be overlooked that he had willingly, according to his statements, 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.'[13]

Hearings

During the first hearing held on 28 November 2023, it was first confirmed that Complainant wanted to proceed with this complaint before the Arbiter in terms of Chapter 555 of the Laws of Malta, and he withdrew his comments[14] in his complaint seeking Arbitration in terms of Chapter 387 of the Laws of Malta. The Service Provider were given opportunity to justify their late reply potentially leading to a state of contumacy.[15]

The Complainant stated:

'I say that it was the first time that I actually used Crypto.com and any transactions with this wallet, and it is something that I have no experience of.

I was advised to invest money in a company who invest in coins. Not in coins like dollar or shekel or in the foreign currency market. And they told me that the company to transfer the money to is Crypto.com so, I opened an account after I saw that Crypto.com is one of the biggest companies in the market. I also saw that they have a lot of advertising in MBA, Teams. And I thought that it was a good institution which will secure my investment.

So, I opened an account, and I started on November 2022 to transfer money. The way to transfer money is from my bank in Israel to Crypto.com. Then I bought USDT, and I transferred these USDT to two main wallets. There was a

[13] P. 123 - 124
[14] P. 4
[15] P. 169 – 172, following this reply contumacy was not enforced.

third wallet in the last transaction but all the money, like around $210,000, was transferred through 25 transactions to two main wallets.

Through this process, I wrote a lot of emails to Crypto.com's Customer Service to help me understand what to do. I received a basic explanation on how to do those transactions. After a few weeks, I tried to withdraw some money back and I succeeded. I thought that everything looked OK.

After a month, I understood that I was scammed by people who stole my money. So, on the very same day, on the 27 December 2022, I wrote an email to Customer Service informing them that all those transactions were a scam and asked them to help me get my money back.

It is important to say that I never received any warnings. Today I know that in the Terms of Use of Crypto.com you can see warning stuff, but nobody warned me, nobody sent an email to tell me that those transactions were dangerous. Or tell me that those wallets were not from familiar exchanges or something. I know this information now, after I investigated the case with Mr Khan's company.

So, I wrote many emails to Crypto.com telling them to help me, maybe to freeze some funds. They rejected all my requests and told me that if the people who stole my money were found, they will help me. If an attorney from Israel will send them emails and tell them to do something, they will do it.

After a month maybe two months, after investigating the case with Mr Khan's company, we got like a map showing how the money got through. Those wallets were two wallets from Crypto.com. I think one was Binance and maybe the other one was OKX.

After we found those wallets, we filed a complaint with the Israeli Police in the Cyber Department and started to send emails to all those exchanges to obtain KYC and information which will help us catch the scammers. So, the Police sent those emails and after a few days we received from the Police that besides Crypto.com, all the rest of the exchanges will co-operate and give us the KYC of the wallet holders.

There was a Chinese citizen and we had someone we actually knew who stole the money. So, I wrote an email to Crypto.com saying, 'Look, we know those

four people who stole my money, and we know that they have their wallets in your company. Please help us get that money back or freeze their assets. Do what you need to do. I do not mean that when the Police will get involved you will help.'

I think it was about a month that the Police were sending emails to Crypto.com who replied back. The Israeli Police told me that they would not co-operate. They did not give us any information and that is how it ends.

That was the situation, so I wrote another letter in March to Crypto.com telling them that I wanted to proceed with my complaint. And they sent me a link to this Arbiter for Financial Services telling me that is the best place to go to file my complaint.

I felt as a person who never used Crypto.com, that Crypto.com expected me to know things which I did not know. How would I know those warnings or how to walk in this world? Crypto.com is such a big company but they have the cheapest damage prevention. This company has all the resources to teach this information to their consumers. The thing is that I did not get any service. I felt like they are telling me, "You lost your money. We are technical; we just move money from one place to another. It's your problem and we have no way to help you."

I spent more money to find out who are the scammers and the Police reaching the company and they still did not want to help me. I do not know, when I want to put money in your company it's OK and when I lost my money, I am the last person you want to help. That was the worst part in this situation. I can tell you that my bank from Israel tried to help and every institution tried to help. Apart from the question of responsibility, one has to help his customer who had spent all his money in your company, and they did not give me any help.'

'Mr Khan confirms that the complainant lost around $200,000 but is seeking compensation for half of his losses. This is due to the fact that they are talking about those transactions amounting above certain thresholds. However, the sum is 200K. The complainant is seeking 100K compensation because of those transactions that fall under a certain threshold which should be followed by the Maltese law according to the regulations that Crypto.com falls under.

Mr Khan confirms that the complainant had lost money only on this Crypto.com platform.'[16]

The cross-examination of the Complainant was held at the second hearing of 22 January 2024, where he said:

'Asked with respect to the transactions complained about whether I authorised these transactions, I say, yes, I wanted to do those transactions.

Asked whether I chose the wallets and the currency, I say that during this process, I try to get help from the customer service so I ask a lot of questions about how I am supposed to do it, how long would it take and ask whether what I am doing is right. These are normal questions from someone who does not know the process.

It is being said that at the time of the transactions, when I was interacting with the customer service staff and with the customer service agent to whom I was asking these questions, I gave them a full impression that I intended to carry out these transactions as well. I asked those questions to verify and to check, to understand that everything was OK. I got the impression that that is the situation, and that I was doing nothing wrong and had nothing to be afraid of.

It is being said that when I was carrying out these transactions, I intended to send money to these people, and since I control the transactions, I knew that I was sending money to people whom I thought were investing for me.

First of all, I say that I did not know these people. I thought that I was investing money in an investing company, so, I do not know those people. But, as in bank transfers, I thought that if I gave the Crypto.com Wallet numbers, they would have a way to check if they were secure and OK. It seemed like a normal situation in exchanges or in banks. I thought that those activities are secure.

It is being said that Crypto.com was not involved in this decision to make this investment and that I was merely using Crypto.com to transfer money.

I say that you asked about my corresponding with customer service before I transferred those money, but, of course, they did not want to invest with me in this company. It was a Crypto.com programme to exchange and transfer money

[16] P. 163 - 166

from each client. Of course, they did not know exactly what I wanted to invest in and what company I wanted to invest in. In my point of view, it is not their job. But I thought that if I move money on this big and famous platform, it would be safe and secure.

It is being said that in my evidence, I complained to Crypto.com of these transactions on 27 December 2022 and the last transaction was on the 20th so it means that I did not complain of the legitimacy of these transactions until I finished the last transfer to these third parties.

I say that in these exchanges I do not know if the Wallets are good or not or if they are associated with these activities.

During the process, I tried to understand myself if there was anything wrong and I used to contact customer service each and every time to get some information. At the end, I understood that this was a wrong investment but during the process, Crypto.com did not help me at all. It did not secure my money or my activity. That's how I felt.

Questions from the Arbiter:

Asked when I was dealing with people from Crypto.com and I was dealing with these transfers, whether I got any assurance that these Wallet numbers were safe to make the transfer, I say no, not at all. What I would like to say is that I did not have a sign that anything was wrong.

During this process, I felt that they were helping me, and I felt that they were giving me a safe road to transfer my money since when transferring money, customer service told me that everything was OK, so I thought that my transfers and my money were safe.'[17]

At the same hearing, the Service Provider presented their proofs and a copy of the Terms and Conditions.[18] Mr Julian Yeung, on behalf of the Service Provider, stated:

'From the evidence that we have at hand, and from the transaction records that we produced, we can see that Mr LD had set up and used his Wallet to withdraw

[17] P. 207 - 209
[18] P. 175 - 206

a total of some 200,795 USDT. This Wallet supports three external addressed Wallets between the 17 November 2022 and 20 December 2022.

In respect of these transactions, we can see that Mr LD himself or someone with his password had access to authorise these transactions. He himself was the one who set up these transactions. Crypto.com merely process these transactions in accordance with his instructions. There is no suggestion that his account was misused by someone else.

It is very clear from his evidence that Mr LD authorised these transactions himself. And based on that, Crypto.com is saying that we are unable to honour the complainant's refund request for the pure fact that these transactions were authorised by himself.

Regarding the allegations that we did not share information, it is very important to understand that when information is requested of us, as a European company, we are subject to the provisions of the GDPR. GDPR which oversees the right to privacy means that we can only respond to legitimate requests from authorities empowered by court orders to request this information from us.

There is a very detailed and very sophisticated system – the International Mutual Assistance Treaty - whereby Maltese companies can request all information from other countries around the world with the Maltese Police. Typically, this is affected through a request to the JAFU or other institutions in Malta.

We never received a request from the Maltese Police, and we never were under the compulsion from a court order to affect any request made by third parties.

Many countries choose to participate in these requests in a different way but, by law, we are not required to give this information for fear of breach of privacy.'[19]

During cross-examination, Mr Yeung said:

'Asked whether we have a transaction monitoring system and, if so, then when Mr LD submitted those Wallet addresses why did they not come up as illicit or a red-light type of Wallet, and why did we give him the OK to transfer, I say that

[19] P. 209

I am very hesitant to give the full details of this because we have to understand that when we talk about transaction monitoring, we necessarily touch upon the potential of STRs which are Suspicious Transactions Reports. I am not allowed by law to define and to declare what the results of those transaction monitoring actions are; whether we have identified anything with the Wallets or not. So, for that reason, I am declining to answer this question. I can tell that Crypto.com does have transaction monitoring which is fully in compliance with the regulatory requirements. I cannot give the details on these transactions for fear of breaching Crypto.com's obligations with the law.

The Arbiter would like to make it clear that this Office is not the proper entity which can enforce any infringement of money laundering obligations. That authority is the FIAU.

Therefore, the Arbiter requests a categoric reply from Mr Yeung is whether their organisation complies with the Implementation Procedures which are imposed on them by the FIAU in so far as monitoring systems are concerned.

The Arbiter refers to Section 2.3 of the Implementation Procedures which details the expectations of the FIAU for the process of transaction monitoring.

Mr Julian Yeung replies:

We comply with all the legal requirements required of us and with the Maltese law, displaying the fact that we have held and maintained this licence that we have for these services. So, yes, the assurance is that we are in compliance with Maltese law.

Asked by the Arbiter whether at the point of enquiry when we were making this transfer did any of the three addresses feature in any warning list which was available to us at that particular time, I say that the way which a transaction operates and with the regulations imposed on us, every transaction is monitored. So, I can say that given transaction was not flagged. If the transaction did not give rise or suspicious rise for us to be suspect of it, then I would say that it does not trigger any of the information available to us.

I say that there is no evidence submitted by Mr LD of all his interactions with the customer service to the extent which says that we gave him an OK for the transfer, I want to clarify that anything that we said with regards to the OK for

the transfer can only be whether or not his instructions can be carried out from a practical point of view not that we can verify or check the transaction as it occurs.

Mr Khan will know in so far as that the recipient address is not one that is held by Crypto.com, we have no obligation to carry out a KYC. We have no obligation to take information of a recipient account. So, to say that our customer service, who would not even have access, something which is very clearly in compliance with the law, to give the OK for the transaction can only ever mean that we see that the transaction fits the practical requirements for being executed.

Asked when the transaction monitoring did happen, whether there is evidence to prove that there were warnings or not while the transaction was being made; and to confirm, submit or disregard the emails sent to us by legal enforcement from Mr LD's side, I say that in respect to Mr LD's request through his legal enforcement's authority, our understanding and our recollection is that Mr LD made the request to the Israeli authorities. The Israeli authorities do not have jurisdiction over a Maltese company.

And as I said in my evidence, Maltese companies can only be bound by law by a Maltese request coming from the JAFU or some mutually recognized EU country. Israel, and the Israeli authorities, would not constitute a reason for us to share this information on the basis of GPDR.

So, I confirm that in so far as this request were made from the Israeli Police, we would have given them information as who the Data Controller is and how to seek that data from us in a proper manner. I have not seen that this was done.

In respect of the first question, I have to remind Mr LD that he carried out transactions in accordance with his instructions. That is all what we are required to do. Crypto.com has no obligation, unlike the bank, to give warnings as to transactions which, on the surface of it, may be suspicious but may be also legitimate transactions. The fact that Mr LD interacted with these Wallets in a regular manner over a regular course of time, would actually give rise that they are regular transactions.

Crypto.com is not responsible for telling their users what are and what are not suspicious transactions. It is for the user to understand whom they are sending

money to. And, by all accounts, Mr LD achieved his purpose; he sent money to the people whom he wanted to send it to. And it is not for Crypto.com to second-guess the purpose of a transaction.[20]

Final Submissions

In their final submissions, the parties largely restated their arguments made in the complaint, the reply and the hearings.

The Complainant concluded that:

'***I respectfully request that you thoroughly review the circumstances surrounding this case and adjudicate in my favor, in alignment with the financial claim I have presented. This claim, I believe, is both reasonable and reflective of my earnest desire for an amicable resolution outside of judicial proceedings. Your consideration towards a fair settlement will be greatly appreciated, and I trust that Crypto.com will engage in the matter with the requisite seriousness and a view towards equitable resolution.'***[21]

The Service Provider concluded:

'***In summary, the Respondent would submit that the Complainant has failed to present a legal requirement on the part of the Respondent to identify the recipient or payee of the Disputed Transaction.***

In addition, the contractual relationship between the Complainant and the Respondent as set out in the Terms and Conditions clearly provides that the Complainant had the responsibility, among others, to verify all transaction information prior to submitting it to the Respondent and to protect his mobile phone from any unauthorized access.

In carrying out these transactions, the Respondent has merely carried out the Complainant's transactions as instructed. On the balance of the foregoing, it is the Respondent's case that the Complainant himself should be responsible for his own alleged losses and that costs should be awarded to the Respondent.'[22]

[20] P. 210 - 212
[21] P. 221
[22] P. 233

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

The Service Provider

Foris DAX is licensed by the Malta Financial Services Authority ('MFSA') as a VFA Service Provider as per the MFSA's Financial Services Register.[24] 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').

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.[25]

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'*. [26]

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...'*.[27]

It offers the account holder *'a crypto custodial wallet'* and *'the purchase and sale of digital assets on own account'*.[28]

[23] Art. 19(3)(d)
[24] https://www.mfsa.mt/financial-services-register/
[25] https://www.mfsa.mt/financial-services-register/
[26] https://crypto.com/eea/about
[27] P. 177
[28] P. 100

Observations & Conclusion

Summary of main aspects

The Complainant made a transfer of his digital assets (USDT) using the *Crypto.com* app. The said transfers were made to three different external wallet address 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 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.

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 the crypto withdrawal once the transaction was done on the blockchain.

<u>Applicable Regulatory Framework</u>

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'*[29] 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[30] also issued Implementing Procedures on the Application of Anti-Money Laundering and Countering the Funding of Terrorism Obligations to the Virtual Financial Assets Sector.[31] 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 US$ 200,000.

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

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 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 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 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 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).[32]

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

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 Instructions for a Digital Asset Transfer to Crypto.com as the Digital Asset Transfer may not be cancelled or reversed once processed …'.[33]

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:[34]

'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.

[33] P. 191
[34] *Ibid.*

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.[35]

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 was 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.[36]

  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

[35] 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).

[36] 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/

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.[37]

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 the strong assertions 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.[38]

The Arbiter also notes the assertion that the Service Provider's alleged failure to provide information to the Israeli Authorities has prejudiced the prospects of recovery of the funds stolen by the fraudsters.

The Arbiter cannot fault the Service Provider for insisting on adherence to their GDPR[39] obligations which provides for disclosure of private information to third parties has to follow the proper process leading to authorisation as stipulated in the GDPR.

[37] 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
[38] p. 210
[39] General Data Protection Regulations – Regulation (EU) 2016/679

Furthermore, the supposition that disclosure of such information could have led to recovery is rather optimistic. Firstly, as explained, the Service Provider had no information on the owners of external wallets recipients of the alleged stolen funds. Secondly, as this particular case shows, even identification of the fraudsters (as is presumably done through the mapping report[40] earlier referred to) does not necessarily lead to recovery.

However, the Arbiter is making a recommendation that could help the authorities to trace the connections of the fraudsters and at least limit their ability to perform further frauds.

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.**

[40] P. 69 - 90

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.[41]

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

Recommendation

The Arbiter notes that according to the folio 78 of the Cryptocurrency Investigation Report and the mapping exercise it contains, there were 5 transactions involving payments of a cumulative, relatively small amount of USDT 2247.65 with the largest being USDT 1,139.43 and the smallest USDT 100. These were transactions effected between 21 November 2022 and 22 December 2022. These being wallets hosted by Crypto.com, Service Provider would have due diligence documents related to the owners of these accounts.[42]

The Arbiter is sending a copy of this decision to the FIAU with a recommendation to investigate the owners of wallet hosted by Crypto.com ending with number 4c72f and share the information with local authorities that are empowered to share such information with Israeli authorities.

Alfred Mifsud
Arbiter for Financial Services

[41] 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.
[42] P. 78

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.