

Before the Arbiter for Financial Services

Case ASF 134/2022

RT ('the Complainant')

vs

Foris DAX MT Limited (C 88392)

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

Sitting of the 10 August 2023

The Arbiter,

Having seen **the Complaint** dated 4 November 2022¹ relating to the Service Provider's alleged failure to prevent, stop or reverse the payment in crypto with a value equivalent to US\$40,500 made by the Complainant from his account held with *Crypto.com* to a third-party who was allegedly a fraudster.

The Complaint

The Complainant explained that on or about 13 November 2021, he fell victim to a multi-layered scam operation orchestrated by an entity referred to as '**Absa Forex**'. He explained that through the services of *Crypto.com* he transferred to this fraudster digital assets USD Stable Coin (USDT) in approximately 47,385 units which he had funded through several transfers amounting to approximately €39,800 made for his debit/credit card to his *Crypto* account.

The Complainant filed an elaborate multi-page (10 pages plus attachments) complaint letter dated 18 January 2022² with the Service Provider in which he

¹ P. 1 - 210

² P. 17 -26

sought full refund of his loss from the Service Provider as he maintains that they are responsibilities for his loss *inter alia* for reasons that the Service Provider:

1. Made his infrastructure available to fraudsters
2. Failed to prevent the illicit transfer of wealth caused by the alleged fraud
3. Failed to perform adequate Anti-Money Laundering (AML) and Know Your Customer (KYC) procedures resulting in onboarding of fraudsters
4. Failed to notice clear signals that the transfer effected by the Complainant to the fraudsters were suspicious and therefore had a duty to warn the Complainant that he was making himself vulnerable to a fraudulent scheme
5. Failed to have monitoring systems to distinguish between normal activity and other activities which are not normal and suggest an illegal enterprise
6. Made negligent misrepresentations about the security of their systems
7. Aided and abetted, knowingly or with severe recklessness, the execution of fraudulent transactions as suffered by the Complainant possible enriching themselves unjustly in the process.

In the Complaint, the Service Provider is often referred to as a Financial Institution and there is an expectation that it should have adopted transaction monitoring systems as required by the EU Payment Services Directive 2 – PSD 2.³

The Complainant sent another letter dated 22 February 2022,⁴ replying to the Service Provider's rebuttal of 8 February 2022⁵ where apart from repeating the original complaints, he concluded that:

"I hereby contend that even given lack of statutory or regulatory obligation on your part to safeguard customers and their funds to the best of your ability, your view nevertheless faces a number of concrete objections:

³ EU 2015/2366 that entered into force 12 01 2016

⁴ P. 8 - 14

⁵ P.15

1. *Your account of the subject matter seems rather incomprehensive as it reprehensibly standardizes (and thus deliberately chooses not to engage) alarmingly unusual conditions; homing in on that which is absolutely indispensable to protect consumers and enhance the integrity of financial systems.*
2. *Suppose I grant, for the sake of argument, that there is no such obligation under the law in any way, shape or form – then your retort would seem quite out of place, given (i) the ease with which you could have forestalled the fraudulent activities depicted herein; and (ii) the increasingly individualized approach that is newly being offered to consumers in view of best industry standards aiming at minimizing financial crime and fraud.*
3. *Your understanding of the role of financial institutions in society is seriously flawed. It certainly does not help to solve the rising problem of online fraud and financial threats that unfortunately go unheeded and unchecked, nor does it show any readiness or willingness to ward off such unlawful activities.*

As one who responsibly approaches this subject with the utmost gravity and objectivity, I am resoundingly confident that there is no available sound foundation for, let alone a persuasive argument in support of, your position.

If despite these objections, my concerns are not appropriately taken into consideration and are instead simply dismissed, you can be assured that alternative action will be taken, and I will make it a point to share our exchanges with the public so that at least pre-emptive action can be taken by other potential clients to avoid any dealings with organizations where customer security is not a priority”.⁶

The Complaint was filed by Complainant with the Office of the Arbiter for Financial Services (OAFS) on 4 November 2022, where he explained:

“I never thought anything like this would happen to me, a moment of inattention and a big the problem arose for me.

⁶ P. 14

Many of my friends recommended that I try dating to find a girlfriend. I tried facebook dating, where the system selected people who fit together. I was in contact with several people and after a few weeks I communicated more intensively with only one of them. She said she works in the financial sector, trades forex and specializes in gold, there is an opportunity to earn extra money in addition to regular employment.

I agreed to try it, she offered to help me set up an account and get instructions on how and when and where to trade.

I downloaded the MT5 pp from the play store (like all the apps I have on my smartphone) and the ABSA broker where I set up an account where I deposited money and traded as instructed. See photo

I deposited \$22,337.88 in my mt5 account. I earned 86020.21 by trading.

I gradually deposited money into the account and traded. When there were \$108,358 in my account, I wanted to withdraw money, and that's when the problem occurred.

I received an email from an ABSA broker, and I was asked to pay taxes \$21,504.88. I paid a tax a little more \$21,506.42, but the crypto.com transaction fee was \$25 so real \$21,481.42 was sent. The tax payment was not accepted by the ABSA trader and I was asked to pay again. I received an email from the money I ignited was transferred to an MT5 account. See photo

All transactions so far have been sent via crypto.com (\$43,819). Other transactions have already been sent via binance.

To prevent problems my 2nd tax pay, I paid a significantly higher amount of \$22,737 (binance) for the next tax payment. The difference between the amount and the tax was credited to my MT5 account of \$1,238.42. Then I was asked to pay 10 percent of the profits as a transaction fee for ABSA broker \$8,601.95.

I paid more \$9,214 (binance) and the difference was credited to my MT5 account (\$610) then I received an email from ABSA trader that I needed to verify the account and send more money. I already understood that I had become a victim of fraud.

A summary of what I paid for

deposit MT5 account \$45,668.39 (deposit for trading \$22,337.88 + first tax payment \$21,481.42 + difference 2nd tax pay \$1,238.42 and difference of 10% fee \$610)

tax \$21,504.88

10% fee \$8,601.95

a total of \$75,775.22 if I count well.”⁷

He explained that he had approached his bank for help to recover the funds and they successfully recovered and refunded €29,500 from the transfers made to his account with Binance Exchange; they did not recover any of the payments made to Crypto.com.

As a remedy, he was expecting compensation for US\$40,500 from Service Provider claiming that they breached the duty of care by turning a blind eye to fraudulent behaviour.

With the Complaint there was attached a letter which the Complainant had sent to OAFS dated 20 October 2022, basically, raising the same issues contained in his complaint letters, referred to above, which he had sent to the Service Provider.

The first report of the suspected scam made to the Service Provider was by email on 3 December 2021. However, the final reply from the Service Provider, in answer to the first formal complaint letter of 18 January 2022, was dated 8 February 2022⁸ which then elicited the second direct complaint letter of 22 February 2022.⁹

Service Provider’s reply

The Service Provider’s official reply dated 6 December 2022¹⁰ stated:

⁷ P. 2 - 3

⁸ P. 15; 202

⁹ P. 8- 14

¹⁰ P. 217 - 227

That *Foris DAX MT Limited* ('Foris DAX' or 'the Service Provider') offers a crypto custodial wallet ('the Wallet') and the purchase and sale of digital assets on own account, through the *Crypto.com* App. The Wallet is only accessible through the App and the latter is only accessible via a mobile device.

That the Complainant became a customer of Foris DAX through the *Crypto.com* App on 12 November 2021 and the alleged fraudulent transactions subject of the complaint, happened between 13 November 2021 and 29 November 2021.

The following timeline was provided by the Service Provider:

- a) On 13 November 2021 Complainant transferred by debit of his debit/credit card €999.86 to his wallet to fund the purchase of USDT 1127 and on same day transferred these USDT (less charges) to an unknown external wallet.
- b) The operation was repeated on 15 November 2021 when Complainant transferred by debit of his debit/credit card €1,987.95 to his wallet to fund the purchase of USDT 2231 and on same day transferred these USDT (less charges) to an unknown external wallet.
- c) The same cycle was repeated in seven other similar transfers by charging his debit/credit card, amounting to €17,324 between 16 November 2021 and 22 November 2021 every time transferring the USDT acquired through the funding to an unknown external wallet.
- d) Finally on 29 November 2021 a transfer of €19,467.99, again by a charge to his debit/credit card, was made to fund purchase of USDT 21505 which was again transferred on same day to an unknown external wallet address.

In total €39,779.80 were transferred and converted into 44025 USDT which were transferred to an unknown external wallet.

The Service Provider submitted that:

“Based on our investigation, the Company is of the opinion that we are unable to honor the Complainant’s refund request based on the facts that the reported transfers were clearly made by Mr RT himself. We have observed no new unique logins and all transactions were executed using Mr RT’s personal login

credentials with two factor authentication (2FA) active. Furthermore, there were no changes to the Complainant's personal passcode through the period between November 13, 2021 – November 29, 2021. This leads us to conclude that the Complainant purposefully funded his Wallet and executed the transfers in his own volition, possibly to seek gains promised by the alleged scammers.

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

While this is an unpleasant scenario, the Company cannot be held liable for the Complainant's conduct, which resulted in him moving his virtual asset holdings to a third party.

As outlined in the Foris DAX MT Limited Terms of Use, which the Complainant has agreed to upon registering an account with Crypto.com, he 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.

Please see the relevant section of the Terms of Use accepted by the Complainant for your reference:

“QUOTE

7. TOP-UPS TO DIGITAL ASSET WALLET AND DIGITAL ASSET TRANSFERS

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. While we fully empathize with Mr RT in this regard, it cannot be overlooked that he had willingly, according to his statements and to the information available on our platform, transferred his USDT virtual asset holdings from his Crypto.com Wallet to external wallet addresses which he had no access to.¹¹

The hearing process

During the first hearing of 14 March 2023, the Complainant stated that he had nothing further to add besides a statement that was presented.¹² Apart from relating personal misadventures that have nothing to do with the case, and quoting an example where Crypto.com was able to recover an erroneous payment in Australia (which has little relevance to this Complaint), the statement emphasised:

1. That Complainant managed to recover payments made on the Binance Exchange but nothing from the payments made to Crypto.com exchange
2. That Service Provider failed him for:
 - a. Lack of transparency
 - b. Lack of consumer education
 - c. Limited customer support
 - d. Lack of insurance

¹¹ P. 226 - 227

¹² P. 240 - 246

The second hearing was held on 29 May 2023. On cross-examination the Complainant stated:

“I confirm that I was the one who authorised each and every one of these transactions through my mobile device.

I confirm that prior to authorising these transactions I was the one who stipulated the withdrawal addresses to which these transfers eventually went to.

It is being said that in so far that Crypto.com is a process transactor for their users, they carried out these transactions accordingly and only to my instructions. I say that yes, it was, but I say that still they are the provider and the expert of the system and I think that if I became a victim of scammers, you need to have an additional system to monitor all transactions.

I confirm that I authorised the transactions believing that I was sending the money to the correct company, not to the scammers.

It is being said that in respect of the transactions, I did not make any complaints about these transfers until the completion of the last transaction. I say that is correct. When I realised that I fell victim of a scammer, I contacted Crypto.com, I contacted Finance and sent my complaint to Finance.

It is being said that at the time that I downloaded the Crypto.com App, I agreed to the Terms and Conditions of Crypto.com’s services. I say that is true.”¹³

The representative from the Service Provider then gave evidence and stated:

“We have already heard the evidence of Mr RT where he has confirmed under cross-examination that he was indeed the one who authorised each and every one of these transactions and, so far as this is concerned, the submissions of the service provider would be that we have merely carried out each and every one of these transactions to his exact instructions.

Mr RT did not raise an objection with any of these transactions until the last of these transactions was completed. Transactions that are concluded and conducted on the blockchain are immutable. That is the very design of these

¹³ P. 254 - 255

transactions; once they are executed and confirmed all across the world by different providers on the relevant blockchain, those transactions are completed. Once the process is initiated it cannot be reversed. That is the whole point of a cryptocurrency transaction: it happens immediately and it is irreversible. Once it's started, the process cannot be reversed.

Crypto.com is unable to provide Mr RT with any reversal of these transactions simply because of the technology; it is not a question of whether we want to or we have to – we are unable to.

Mr RT has brought on examples of other exchanges, such as Binance, in his submissions but he has not actually substantiated any of this with evidence other than his bare assertion.

Each cryptocurrency exchange carries out their processes according to the licencing authorities which they operate from. Today we are concerned with Foris DAX MT which is a Maltese-licenced exchange and we are concerned with the Maltese regulations at hand.

Mr RT has not presented us with any evidence that Crypto.com which operates as Foris DAX MT has offended any of the laws or any other regulations which it is obliged to obey. We also have no evidence about the transactions which were carried out on these other exchanges and therefore we cannot apply into circumstances which Mr RT has occurred on other exchanges. All we can talk about today is what happened on our system. On our system each and every one of these transactions was to an external Wallet which we have no control over.

The complaints were made late after the transactions had occurred. And, as such, we, at the same time, could not have possibly reversed any of these transactions that Mr RT complains about.

Finally, if we look at the Terms and Conditions of the Crypto.com App, in particular at Clause 7.2, which makes it very clear that because of the technology surrounding cryptocurrency, the users themselves are the ones responsible for authorising, validating and confirming the legitimacy of the transactions which occurred, and that is precisely because of the reasons that I have just set out.

Once put into action, these transactions cannot be reversed in so far as they are transactions which occur on the blockchain. Transactions which occur on the blockchain involve one of our Wallets with an external Wallet which is not under our control. And that is precisely the situation that has occurred in these transactions and in these circumstances.

Whilst we sympathise with Mr RT, and he may well have been a victim of a scam, (we cannot confirm or deny that), he simply authorised us to carry out transactions, and we simply carried out the transactions faithfully to his instructions.

On these occasions we are not here to be responsible for having carried out exactly what we had set out to do, which is to carry out Mr RT's specific instructions in each one of these transactions".¹⁴

On being cross-examined, the representative of the Service Provider stated:

"I say that in respect of the complainant's transactions so far as they were carried out by him, in so far that they were authorised by the complainant and in so far as each and every transaction passed two-factor authentication, they were not considered to be suspicious transactions.

Added to this fact, is that these transactions were carried out over a course of time. There were in total almost ten transactions and they were carried out over the course of two weeks.

For those reasons they were not flagged in our system as being suspicious.

I say that we use a number of vendors who provide us with daily updates.

We would like to point out that there are millions upon millions upon millions of cryptocurrency addresses. We are already updating our databases on a daily basis and we rely not only on our efforts but the efforts of third parties.

So, for the complainant to say that he was not protected by Crypto.com is an absolute sham. His transactions were carried out through one of the highest secure cryptocurrency App in the world. I think our security qualifications speak for themselves. We are the only company in the world that has the

¹⁴ P. 255 -257

qualifications that we do. That includes, for instance, Level 321 Compliance for PCITSS and various ISO qualifications. What I would like to say is that we have a robust system.

In spite of having said that, Mr RT has not provided any legal basis for his complaint. He is merely complaining that he believes that we have carried out his transactions and these security features and all I can say is that we have.¹⁵

Upon being questioned by the Arbiter about the first time that the Complaint was raised after the 29 November 2021, the Service Provider said that the first letter dated 18 January 2022 was sent to them only on 4 February 2022, almost two and a half months after the last transaction (subject of the Complaint) was executed.

The Complainant said:

“It is true because after the New Year, I realised that I had become a victim of a scam. I did not do anything for a month because I thought I lost all my money. After the New Year, I spoke with my friend and he told me about a company on the internet that could help me get my money back and I had to do something about that. So, I contacted Crypto.com in January when I filed a complaint with Crypto.com and Binance as well; and after a few weeks I received the answers. Binance retrieved my money but not Crypto.com.

The Arbiter is asking me if I have any evidence corroborating my allegation that Crypto.com and the unknown external address may know each other or do business together, I say, I don’t know; but I think that because I sent money to that wallet to Crypto.com, I download that application MT4 from my mobile phone from the Store, I would never think that it was the scammers.¹⁶

In reply, the Service Provider declared:

“I think that we can come out explicitly and on record that the external wallet address has nothing to do with us. And nor has the complainant advanced any evidence of such”.¹⁷

¹⁵ P. 257

¹⁶ P.258

¹⁷ ibid

The Arbiter then requested the parties to make final submissions which on the part of the Complainant should include evidence that under similar circumstances another Exchange refunded €29,500 to the Complainant of the funds transferred to the same scammer. This would appear to challenge the concept that transactions on blockchain cannot be undone once executed. The Service Provider will then give his reply in their final submissions.

The final submissions

In the final submission filed by the Complainant on 26 June 2023, he submitted evidence of a credit of €29,500 credited to his bank account with TATRA BANKA (Swift Code TATRSKBXXX) on 18 May 2022 that related to refund of settlement on 6 December 2021.

To explain such refund, TATRA BANKA submitted an explanation letter stating:

“Despite the fact that these are not unauthorized transactions, i.e., you do not question the execution of the transactions, you have the right to ask the bank for cooperation in resolving the dispute with the merchant. Through verification, we found that these are approved (authorized) transactions, in which the bank acts only as a clearing agent, that is, it is responsible for its correct settlement. However, the bank is not responsible for the positive processing of the cardholder’s request for the return of the transaction, if the conditions for its execution have been observed.

The holder of the payment card does not have an automatic right to the return of funds from the payment made with the payment card, if the merchant’s authorization to settle the payment is proven, or if he otherwise proves that he is not obliged to return the payment.

For the sake of completeness of information, we state that we are not authorized to resolve any disagreements between the merchant and the cardholder that arose in connection with the ordering of goods or services, or the return of payment and the quality of purchased goods/services provided. In this case, the contract is established between the cardholder and the merchant.

Despite the above, we have contacted the foreign merchant bank with a request to investigate the situation and return the claimed transactions. They partially accepted our request, so in the coming days we will credit the amount of the

claimed transactions in the total amount of EUR 29,500.00 (5 x EUR 5,000.00, 1 x EUR 3,500.00 and 1 x EUR 1,000.00) to your current account.

We attach the documents to the rejected transactions that we received from the merchant bank “CRO INTERNET” in the appendix of this answer.

At the same time, we inform you that the transactions in question were carried out on the basis of confirmed consents in accordance with the agreed conditions. For the stated reasons, we are not entitled to continue in an international complaint procedure with a merchant’s foreign bank.

Thank you for your understanding and for accepting this information.”¹⁸

The accompanying statement indicates payments made to Binance being five payments of €5,000 each, one payment of €1,000 and one payment of €3,500 (€29,500 in total all effected between 30 November 2021 and 02 December 2021), immediately after the last payment transfer made to Crypto.com. It also includes all the payments referred to earlier made to Crypto.com between 13 November 2021 and 29 November 2021.

The submissions also included a copy of a communication from Binance to the Complainant dated 23 March 2022 wherein Binance state as follows:

“Withdrawal Suspended from Fraud/Chargeback

We received a fraud/chargeback report of your card purchase with <cardBin:440577, cardLast4:6084> on our platform, your account withdrawal function has currently been disabled. Due to the violation of our Terms of Use, we have taken a tough decision to terminate the service.

In order to withdraw the remaining funds in your account, we would like you to submit an appeal with the link below. You may either need to choose between returning the dispute amount to spot wallet for deduction, or cancelling the dispute request with your card issuer in this appeal. This link will last for 180 days, your account will be automatically disabled if we have not received any appeal response from you after this period.

Appeal Link: <https://www.binance.com/en/my/risk/fraud-chargeback-appeal?>

¹⁸ P. 280

Id=2022032300030149201641321

Don't recognize this activity? Please reset your password and contact customer support immediately.”¹⁹

In their final submission, the Service Provider, apart from repeating the earlier position that the Complainant is fully responsible for his loss due to gross negligence, states as follows relating to the recovery by Complainant of the payments made to Binance through the chargebacks raised by TATRA BANKA:

“In his Final Note of Submissions, the Complainant has alleged he had received a refund from Binance and submitted a number of documents to support his claim.

The email from Binance dated 23 February 2022 (page 262-263 Complainant's Final Note of Submissions) and screen captures of what is purported to be Binance's Bank Notification Appeal (pages 267 to 271 of the Complainant's Final Note of Submissions) are the only documents from Binance that the Complainant has filed as evidence.

The Respondent would first highlight that the response from Binance dated 23 February 2022 is a standard email that is sent to customers of Binance when a fraud/chargeback report has been made. It is submitted that his email and the decision to terminate the Complainant's account with Binance was sent to the Complainant in response to the Claimant's bank (Tatrabanka) filing a fraud/chargeback request with Binance.

As a result of the fraud/chargeback request from Tatrabanka, it can be seen in the same email that Binance had restricted the Complainant from withdrawing the remaining funds in his Binance account until he either 1) returned the disputed amount to his Binance account for deduction; or 2) cancelled the dispute request by way of submitting a Bank Notification Appeal, the link for which is included in this email.

The Bank Notification Appeal for Binance lists the transactions the Complainant has disputed as follows:

- i. 5,000 EUR 2021-11-30***

¹⁹ P. 263

- ii. 3,500 EUR 2021-12-02**
- iii. 5,000 EUR 2021-11-30**
- iv. 1,000 EUR 2021-11-30**
- v. 5,000 EUR 2021-12-02**
- vi. 5,000 EUR 2021-11-30**
- vii. 5,000 EUR 2021-11-30**

29,500 EUR (Total)

The Deduction Agreement that can be found in the Bank Notification Appeal states the following:

- i. You agree to return the relevant dispute amount in BUSD to your wallet before submitting this appeal.**
- ii. Binance has the consent from you to deduct the relevant dispute amount in your spot wallet account.**
- iii. Once the deduction of the dispute amount has been made, your account withdrawal function will be restored for 3 days for you to withdraw the remaining assets, thereafter your Binance account will be closed.**

It is submitted that the two documents filed by the Complainant do nothing to support his claim that Binance refunded the funds which the Claimant disputed. In fact, these two documents contradict the Claimant's assertions and only goes to show that upon receiving a fraud/chargeback report from the Complainant's bank, Binance proceeded to terminate the Complainant's account and restrict any withdrawals of his remaining balance until the Complainant either returned the disputed amount to his Binance account or withdrew his fraud/chargeback report. There is no mention by Binance of any successful retrieval or refund of the EUR 29,500 that is the subject matter of the fraud/chargeback report.

The Respondent submits that the screen captures of the Complainant's Tatra Banka transactions on page 264 of the Complainant's Final Note of Submissions do not show the name of the bank or account holder from which the deposit of EUR 29,000 on 18 May 2022 has come from. Even if it is to be assumed that this deposit originated from Binance, the Respondent would submit that on the

evidence that has been presented to the Arbiter, it cannot be concluded that the payment was pursuant to a refund or monies recovered by Binance.

Finally, it is stressed that even if the Arbiter finds it to be the case that Binance had indeed refunded the Complainant's funds, this is far from establishing a legal basis for the refund itself.²⁰

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 Transactions or to second guess or challenge the Complainant's express and accurate instructions.

Furthermore, and in any case, the facts of the case and the nature of the transactions did not give rise to any reasonable suspicions as to their legitimacy and neither has the Complainant adduced any cogent evidence to suggest that the Complainant would have stopped from proceeding with the Disputed Transactions had he been warned not to effect them, particularly when it is now apparent that the Complainant was executing similar transactions with other service providers at the same time of the Disputed Transactions.

Ultimately and as established in the Terms and Conditions of the Crypto.com App to which the Complainant expressly agreed to at the time it signed up for the Respondent's services, it is for the Complainant to bear the burden of verifying all transaction information prior to submitted counterparties they transact with. The Respondent has merely carried out the Complainant's express instructions at all material times as such, bears no responsibility for the alleged consequences of the Disputed Transactions.²¹

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

Further Considers:

The Merits of the Case

²⁰ P. 286 -287

²¹ P. 287

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 555²² 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.²³ 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.²⁴

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*”.²⁵

The Application

*“Foris DAX MT Limited (the ‘Company’) offers the following services: a crypto custodial wallet (the ‘Wallet’) and the purchase and sale of digital assets on own account. 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.”*²⁶

Observations & Conclusion

Summary of main aspects

²² Art. 19(3)(d)

²³ <https://www.mfsa.mt/financial-services-register/>

²⁴ <https://www.mfsa.mt/financial-services-register/>

²⁵ <https://crypto.com/eea/about>

²⁶ P. 217 & 285

The Complainant made a transfer of his digital assets (BTC) using the *Crypto.com* app. The said transfer was made to an external wallet address allegedly used by a fraudster. The transfer was in respect of a fake trading platform which the Complainant claimed was a scam.

In essence, the Complainant is seeking partial reimbursement from Foris DAX for the Service Provider's failure to prevent, stop or reverse the payment he made to the fraudster. He is seeking as remedy a refund of USD 40,500 which he claims is a refund of his losses through transfer to *Crypto.com* from his debit/credit card amount to €39,779.80.

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.

Applicable Regulatory Framework

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

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

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

The Arbiter further notes that in the year 2020, the MFSA has also issued a “*harmonised baseline guidance on Technology Arrangements*”²⁷ 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”).

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 an external wallet from his crypto account. At no stage has the Complainant raised any doubt as to his having authenticated the transactions personally.

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

- The Complaint involves a series of payments made by the Complainant from his account held with Foris DAX, to an allegedly fraudulent external trading platform causing a loss to the Complainant of €39,779.80.

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

²⁷ Guidance 1.1.2, Title 1, “*Scope and Application*” of the “*Guidance on Technology Arrangements, ICT and Security Risk Management, and Outsourcing Arrangements*”.

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 himself had “*whitelisted*” the address giving the all clear signal for the transfer to be executed. In fact, the Complainant himself dismissed that he had 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 more than two months after execution of the last of the disputed transactions were already executed and finalised.²⁸

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).²⁹

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

²⁸ Crypto transactions may be processed and completed within a few minutes or hours (as indicated on various websites following a general search on the internet).

²⁹ 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 ...”.*³⁰

On the basis of the facts presented during the case, the Arbiter could not conclude that the Service Provider failed to adhere to any specific obligation, or any specific regulatory requirements applicable to it, nor did he find any infringement of the Terms and Conditions applicable in respect to the service offered.

It is noted that in his formal complaint to the Service Provider, the Complainant only referred in a general manner to the regulations and standards applicable to Foris DAX “*financial institution*”.³¹ In the said formal complaint reference was also made to “The Federal Trade Commission (FTC) Act, 15 U.S.C.”,³² enacted in the USA.

However, these are not considered applicable also given that the Service Provider is not “*a licensed and regulated financial institution*”. Foris DAX is only regulated and licensed as a VFA Service Provider based in Malta as outlined above.

The regulatory regime applicable to a VFA Service Provider is indeed a different one and does not necessarily reflect the requirements and consumer protection measures applicable to a financial institution falling under EU regulatory regimes.³³

Indeed, if the Complainant is seeking protection 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 transfer to his Crypto account.

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

³⁰ P. 226 - 227

³¹ P. 19 & 22

³² P. 19

³³ 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).

- **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.³⁴

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

A person who chooses to venture into the area of crypto which, itself, is typically a highly speculative and risky market, needs to also be highly conscious of the potential lack of, or lesser, consumer protection measures applicable to this area of business, as compared to those found and expected in other established sectors of the financial services industry. EU regulatory bodies have issued various warnings to this effect over the past years.³⁵

The issue of refund from Binance

³⁴ 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 2023 / 2024 – <https://www.financemagnates.com/cryptocurrency/can-mica-take-europe-to-the-crypto-promised-land/>

³⁵ 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

In his Complaint the Complainant raised the point that when he asked for support from his Bank to help him recover the funds:

“they contacted Binance Exchange, and we were able to successfully recover the amount that went through Binance (€29,5000) unfortunately I didn’t have that luck with Crypto.com, they failed to provide me with a positive resolution, which disturbs my peace of mind into thinking that Crypto.com is willingly allowing malicious behaviour under their network and refusing to accept responsibility for what happened to me”.³⁶

This gave a first impression that Binance refunded what Crypto.com are refusing to refund and seemed to challenge the assertion that transactions on blockchain cannot be reversed once executed, or that Binance have actually refunded the amount out of their own pocket.

However, evidence provided by the Complainant shows that the refunds were the result of card payments chargebacks which were consented to the Merchant’s (Binance) bank but were in fact challenged by Binance to the extent that they blocked their client account.³⁷

As TATRA BANKA say in their letter:³⁸

“The holder of the payment card does not have an automatic right to the return of the funds from the payment made with the payment card, if the merchant’s authorization to settle the payment is proven, or if he otherwise proves that he is not obliged to return the payment.”

And in relation to the lack of success of chargeback claims with the merchant bank of Crypto.com they state:

“at the same time, we inform you that the transactions in question were carried out on the basis of confirmed consents in accordance with the agreed conditions. For the stated reasons, we are not entitled to continue in an international complaint procedure with the merchant’s foreign bank.”

³⁶ P. 4

³⁷ P. 263

³⁸ P. 280

It is clear from the above, that the success in refunds of payments made by card payment to Binance is not the result of a refund by Binance but the result of success of the chargeback claims made by the Complainant's bank with the Merchant's bank clearing Binance's card payments. The same success did not result in case of card payments to Crypto.com.

As there is abundant clarity that the payments to Service Provider were all fully authenticated by the Complainant, there is valid explanation why the chargeback on Crypto was not successful.

The Arbiter has no visibility on the reason why the Merchant Bank clearing payment to Binance has authorised the chargeback, in full disagreement of Binance, but this in no way challenges the case made by the Service Provider that payments made on blockchain once executed are irreversible.

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 than 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.³⁹

Given the particular circumstances and novel nature of this case, each party is to bear its own legal costs of these proceedings.

**Alfred Mifsud
Arbiter for Financial Services**

³⁹ 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.