

Before the Arbiter for Financial Services

Case ASF 009/2023

GH ('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 20 January 2023¹ relating to the Service Provider's alleged failure to prevent, stop or reverse the payment in crypto with a value equivalent to €42,366 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 12 October 2021, he fell victim to a multi-layered scam operation orchestrated by an entity referred to as '**FiniTrend**'. He explained that the equivalent of €42,366 were transferred from his wallet, utilizing the services of *Crypto.com*, to this scammer.

The Complainant filed an elaborate multi-page (10 pages plus attachments) complaint letter dated 3 February 2022² with the Service Provider in which he

¹ P. 1 - 51

² P. 7 -16

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 17 March 2022,⁴ replying to the Service Provider's rebuttal of 15 March 2022,⁵ 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. 33 - 40

⁵ P. 19

- 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 20 January 2023 basically repeating the same issues made in the original complaint to the Service Provider and attaching a letter dated 4 July 2022⁷ that Complainant had sent earlier to OAFS which had concluded:

⁶ P. 39 - 40

⁷ P. 25 -31

“Based on my analysis, and as confirmed by various authorities concerned with such matters, there is abundant evidence that forward-thinking financial institutions ought to take reasonable steps to forestall fraud, or at least mitigate its risk by using an effective risk management system, demonstrating their undisputed ability to responsibly and pre-emptively respond to questionable transactions in the digital arena. The use of such systems, largely based on newly adopted technologies aimed at effectively navigating the evolving threat landscape, is only one of a number of possible endeavours undertaken in this connection, alongside the application of past knowledge and experience related to popular fraudulent practices.

Astonishingly, I am pondering how it is that, despite being shown that Crypto.com’s business conduct was insufficient insofar as background checks are concerned, they keep refuting their indisputable role and responsibility in connection with the matter herein discussed. The points that I have hitherto made are too crucial to be taken lightly. Crypto.com’s non-observance of the fundamental principles of justice – that is, to completely overlook and not even remotely try to mitigate the suffering of vulnerable consumers – is inexcusable given the size of the establishment and the vast resources at its disposal as the direct result of the patronage of clients like myself.

If it was, indeed, solely my responsibility, we must then believe at least one of the following clauses: a) financial institutions have absolutely no role whatsoever in preventing and detecting fraud, b) the fraud in question was not reasonably foreseeable, or c) the transactions in question were not sufficiently alarming. It is extremely unfortunate that Crypto.com pushes quite hard for me to believe all three of these things – despite evidence to the contrary.

In summary, I respectfully ask your organization to consider my points, given your personal and companywide obligation to provide a fair and reasonable investigation into the complaint.

I look forward to your input and would gladly cooperate to reach a fair and reasonable outcome.”⁸

⁸ P. 31

However, in his official Complaint, the Complainant sought a lower remedy than what had been sought in the direct complaint to the Service Provider.

“I need to get 50% back to my account (Compensation).”⁹

And in reply to what remedy he is seeking, he simply stated:

“20,000 EUR”.¹⁰

Service Provider’s reply

The Service Provider’s official reply was received on 26 January 2023¹¹ stating 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 08 October 2021 and the alleged fraudulent transactions subject of the complaint, happened between 12 October 2021 and 11 November 2021.

The following timeline was provided by the Service Provider:

- a) On 12 October 2021 Complainant bank-transferred €6,850 to his wallet and on same day converted these to Bitcoin (BTC) which were then transferred on the same day to an unknown external wallet.
- b) The operation was repeated on 18 October 2021 when Complainant bank-transferred € 15,000, converted same into BTC and again transferred then out to an unknown external wallet on the same day.
- c) The same cycle was repeated in five other transfers amounting to €20,516 between 22 October 2021 and 11 November 2021 every time transferring the BTC acquired through the funding to an unknown external wallet.

⁹ P. 2

¹⁰ P. 4

¹¹ P. 57 - 78

In total €42,366 were transferred and converted into 0.7808428 BTC which were transferred to an unknown external wallet. The average acquisition price of BTC was €54,257.

It is not clear when Complainant first contacted the Service Provider with his complaint. However, the first rebuttal of the Service provider dated 15 March 2022 states:

“We apologize for the delay in getting ack to you. It appears that your initial request from a month ago was not properly escalated”.¹²

This seems to refer to the official complaint of 3 February 2022 above referred to.

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 fact that the reported transfers were clearly made by Mr GH 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. All transactions were executed using Mr GH’s personal login credentials. Furthermore, there were no changes to the Complainant’s personal passcode or email address through the period between October 12, 2021 – November 11, 2021.

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

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

¹² P. 19

Mr GH 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 GH 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 an external wallet address 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.

We remain at your disposal for any further information you may require pertaining to the above case”.¹³

The hearing process

The first hearing was scheduled for 18 April 2023, but Complainant excused himself at the last minute and the hearing was rescheduled for 16 May 2023.

Complainant stated:

“My case is that I am a victim of a fraud that started in September 2021, when I was approached by a company called FiniTrend. I have submitted many emails I started to invest in crypto and I sent money to Crypto.com that was then invested into crypto with this company called FiniTrend. Of course, it was a fraud, and they kept the money. I understood that in October, so it was about two months into the trading. I roughly estimate that I lost about €42,000.

Then, suddenly, when they understood that that was my limit and I would not get any further, I could not get in touch with them. So, I understood that I was a victim of a fraud, so to say.

I tried to contact them via their website which was very professional, which brought me to believe in them. It all started by an ad on the internet; and it is two years since this happened. I was contacted by them; I started to see their ads on the internet. I think it was on YouTube that frequently just came up with films and ads and they looked very professional. I investigated them: I tried to read about them in news articles in English papers and they had a good resume. I also checked on Trust Pilot where it was mentioned that they were honest and doing a good job. So, in the end, I started to invest via this company called FiniTrend. The man I talked to all the time was Andy Blake. I also tried to call him just to verify; they picked up the phone when I called, and this was an English number with a land code 44. He spoke very good English, and I also spoke to a man who, they said, lived in Switzerland. I do not know his name though because I only spoke to him once. He was also very fluent in English.

Then, when I tried to take money out, it was neglected; and on their homepage it said that it was pending. And that is where it all stopped. They did not answer

¹³ P. 64 - 65

my phone calls, they did not answer my mail. They did not do anything; they were just gone.¹⁴

When asked by the Arbiter if he had any suspicion or evidence that there is a link between Foris DAX and this fraud company FiniTrend, the Complainant replied:

“no, I do not have a suspicion that they are connected in any way. The only thing I know regarding this is that it does not say when the money was taken out of Crypto; it does not say who took the money. It was just a lot of figures: numbers and letters in combination. That is all I know. I do not know where the money went from Crypto.”¹⁵

On cross-examination, the Complainant confirmed:

“I confirm that it was me who opened the crypto account. I also confirm that it was me who made the Euro deposits between the 12 October and 11 November 2021, by a German bank called N26.

I confirm that subsequent to the deposits, I also converted the Euros into Bitcoin.

I confirm that after I converted the Euros into Bitcoin, I made withdrawal orders to send these Bitcoin to an external Wallet address who I believed in. Otherwise, I would not have done that.

Asked who gave me the external Wallet address to send the Bitcoin to, I say that it was Andy Blake.

Asked whether I recall whitelisting this external Wallet address in my Crypto.com account, I say that when the transaction was done it was not eight numbers or something like that. It was not a long, long list of letters and numbers. It was like a bank account number; just numbers, no letters.

It is correct to say that when I made the withdrawal orders, I inputted the numbers which Mr Blake gave me.

It is also correct to say that these withdrawals were successful.

¹⁴ P. 80 - 81

¹⁵ P. 81

I confirm that I have included screenshots of each withdrawal in my complaint to the OAFS.

I confirm that the withdrawal address is the one that I inputted when I was sending Bitcoin to Andy Blake by inputting these series of numbers. I remember six/eight/ten numbers. They were only numbers.

I am being referred to page 47 of my complaint where there is a screenshot of a withdrawal of 0,2761898 Bitcoin. I confirm that this is a screenshot I took from my account, and that it was a withdrawal made on my instructions and that it was correctly handled by Crypto.com in accordance with my instructions. I say that everything has been according to my instructions when it comes to Crypto.com.”¹⁶

A second hearing was held on 6 June 2023 where the Service Provider presented their defence.

They stated:

“The transactions complained of in this immediate case stretched back from 12 October 2021 to 11 November 2021, where numerous amounts of purchases, exchanges and withdrawals of cryptocurrency were made.

In the evidence of Mr GH, we heard that he invested with a company called FiniTrend. Upon hearing of FiniTrend, he himself had performed his own research including with a third-party Trustpilot and, after verifying that they were a trustworthy partner or investment platform, he decided to perform his investments. On the evidence of Mr GH himself, he tells us that he had opened the account; he was the one who conducted the transfers and withdrawals. The transactions that he complains of were actually completed according to his express instructions.

From our side, we would say that from our records and from what we can see ourselves, there is no reason to suspect that any other person than Mr GH himself had performed these transactions. There were no login changes; there were no suspicious circumstances, and neither were there any reasons for us to

¹⁶ P. 81 -82

suppose that these transactions were not intended by Mr GH to be performed in this manner.

According to our Terms and Conditions of the service provider, you yourself, as the user of the platform, are responsible for the validity as well as the authenticity of the transactions you make. In this case, we would say that Mr GH has admitted that he was the one who performed the transactions and that the transactions were performed in accordance with his instructions. And he himself has to bear the consequences for those withdrawals.

On the balance, we would say that the service provider is not responsible for the subsequent events that happened after withdrawal; and we should not be at fault merely because we conducted the transactions in accordance with Mr GH's specific instructions".¹⁷

On cross-examination, the Service Provider stated:

"Asked where the complainant's money went when it left his account with us, I say that when the complainant made a withdrawal, he indicated a withdrawal address. The withdrawal address represents a blockchain wallet which holds or is capable of holding cryptocurrency or other digital assets. The withdrawal that he made is also something that can be independently verified through various tools on the internet that one can find for free.

I can say that in our response filed with the OAFS, after each of these withdrawals we provide what we call 'the transaction blockchain link'. He can see from those links where the cryptocurrency went to; and it went specifically to the wallets which he designated.

Having said that, we are unable to tell the complainant who the owners of these wallets are. Crypto.com only performs Know Your Customer or Know Your Business checks on its own customers, such as the complainant, and it does not and is not obliged to perform identity checks on the identities of third-party wallets. So, he has to find out whether or not this wallet is hosted by another service provider – what we call 'centralised exchange' – or, in the event that it is hosted by a non-centralised exchange, I do not believe that anyone would necessarily have the ability or the tools to track exactly who has or who was the

¹⁷ P. 111-112

person behind that wallet. This is an investigation that unfortunately the complainant has to do himself.”¹⁸

On being questioned by the Arbiter, Complainant confirmed that funds transferred came from his bank in Sweden to a bank in Germany where he had an account ***“the N26. The money that came to Crypto came from N26 in Germany”.***¹⁹

Final Submissions

The Complainant informed he had no further submissions to make.

The Service Provider repeated the claims of gross negligence on the part of the Complainant and concluded:

11. “On the balance of the foregoing, it is the Respondent’s case that the Complainant should be responsible for any losses which occurred out of his own gross negligence. While the Complainant appears to have fallen victim to a scam, there is no dispute that he himself had personally authorized the BTC withdrawals. The Respondent had no cause to believe that the Disputed Transactions were improper and has merely carried out the Complainant’s express instructions.

12. In summary, the Respondent would submit that the Fraudulent Transactions were carried out by the Complainant, and it was the direct result of the gross negligence of the Complainant.”²⁰

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

¹⁸ P. 112

¹⁹ P. 113

²⁰ P. 120

expedite the decision as he is obliged to do in terms of Chapter 555²¹ 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.²² 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.²³

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*”.²⁴

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...*”.²⁵

It offers the account holder “*a crypto custodial wallet*” and “*the purchase and sale of digital assets on own account*”.²⁶

²¹ Art. 19(3)(d)

²² <https://www.mfsa.mt/financial-services-register/>

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

²⁴ <https://crypto.com/eea/about>

²⁵ P. 86

²⁶ P. 57

Observations & Conclusion

Summary of main aspects

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 reduced the original claim for full refund of losses to €20,000 (being about 48% of his total loss) thereby seeming to admit an element of contributory negligence.

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 €42,366.

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 late on 3 February, nearly three months after 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

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:³¹

“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”.

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 *“as a licensed and regulated financial institution”*.³² In the said formal complaint reference was also made to *“The Federal Trade Commission (FTC) Act, 15 U.S.C.”*,³³ 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.

³⁰ P. 99

³¹ *Ibid.*

³² P. 9; 12

³³ P. 9

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.³⁴

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.

- **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.³⁵

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

³⁴ 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).

³⁵ 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/>

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.³⁶

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.

³⁶ 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

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.

In fact, the Arbiter notes that apart from the fraud aspect of this loss, Complainant bought into BTC at quite peak prices and, fraud apart, he would still be nursing considerable investment losses.

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.³⁷

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

³⁷ 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.