

Before the Arbiter for Financial Services

Case ASF 118/2022

AF ('the Complainant')

vs

Foris DAX MT Limited (C 88392)

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

Sitting of 10 August 2023

The Arbiter,

Having seen **the Complaint** dated 5 October 2022¹ relating to the Service Provider's alleged failure to prevent, stop or reverse the payment in crypto with a value equivalent to US\$ 15,000² 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 14 February 2022,³ he fell victim to a multi-layered scam operation orchestrated by an entity referred to as "**Tradevalue Pro**". He explained that the equivalent of US\$ 15,000 were transferred from his wallet, utilizing the services of *Crypto.com*, to this scammer.

The Complainant filed an elaborate multi-page (11 pages plus attachments) complaint letter dated 29 March 2022⁴ with the Service provider in which he

¹ P. 1 - 113

² The Complaint was registered for US\$ 15,000 being approximate market value of digital assets (ETH) on date of transfer to alleged fraudulent wallet in February 2022. In the course of the proceedings, it resulted that the actual transfers made in the period of the alleged scam were valued by Service Provider at €7,063.39 as at 13 October 2022, being between the date of the Complaint and the date of the Service Provider's reply.

³ Effectively, the transactions of alleged fraud were executed in two batches, one on the 14 February 2022 and then on 21 February 2022.

⁴ P. 6 - 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 on-boarding 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 2.⁵

The Complainant sent another letter dated 1 June 2022 to the Service Provider in reply to their original response negating their responsibility 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:

1. *Your account of the subject matter seems rather incomprehensive as it reprehensibly standardizes (and thus deliberately chooses not to engage)*

⁵ EU 2015/2366 that entered into force on 12.01.2016

alarminglly 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 Service provider replied definitively on 4 July 2022⁷ stating:

“Dear Mr AF,

Thank you for your patience while we had your rebuttal letter fully looked into as well. Having performed an independent review of the situation, I would unfortunately need to advise you that our final stance on the matter remains the

⁶ P. 80

⁷ There were earlier exchanges seeking more information from Complainant

same and we will not be in position to offer any reimbursement. I would like to clarify that this decision is in no way personal and is fully in line with our Terms and Conditions, as outlined in one of my previous emails. I fully appreciate this will probably not be a satisfactory outcome for your complaint and we would fully respect your right to escalate the matter outside of our company as well.

Should we be contacted externally, we will cooperate.

With that said, I would still like to urge you to file a report with the Police authorities and have them check in with us in regards to any internal information they may need during the course of their investigation via email address lawenforcementglobal@crypto.com and our relevant team will be happy to assist.

Kind regards,

The Crypto.com Team

Foris DAX MT Limited – External complaints handling.process.pdf.”⁸

The Complaint was filed by Complainant with the Office of the Arbiter for Financial Services (OAFS) on 5 October 2022 basically repeating the same issues made in the original complaint to the Service Provider and attaching a letter dated 13 September 2022⁹ that Complainant had sent earlier to OAFS which had concluded:

“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.

⁸ P. 36

⁹ P. 38 - 44

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.

*Thank you.*¹⁰

Service Provider's reply

The Service Provider's official reply was received on 31 October 2022¹¹ 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 10 January 2021, and before the alleged fraudulent transactions subject

¹⁰ P. 44

¹¹ P. 119 - 142

of the complaint, he had made various transactions on his account which included the transfer from an unknown external wallet digital asset Ethereum (ETH) in units valued at €11,151.31 on 31 December 2021.

The following timeline was provided by the Service Provider:

- a) On 14 February 2022 Complainant made six transactions whereby he transferred to an unknown external wallet ETH units then valued at €4,533.90
- b) On 21 February 2022 Complainant made six transactions whereby he transferred circa 3.3936 units ETH at the time valued at about €7,720 to an unknown external wallet. The ETH units were funded by exchanging other digital assets in Complainant's portfolio and by transfer of GBP 2,720.09, GBP 862.74 and €1,205.78

A copy of the communication between the *Crypto.com* Complaints Team and the Complainant when the Complainant initially contacted Crypto on 21 February 2022 (same day as the last batch of above-mentioned transfers out to an unknown external wallet) was provided by the Service Provider,¹² and at one point Complainant admits:

"I've been so stupid".¹³

The Service Provider submitted that:

"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 had agreed to upon registering an account with Crypto.com, he is solely responsible

¹² P. 183 - 184 FS-3

¹³ P. 184

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 AF 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.”¹⁴

The hearing process

The first hearing was held on 30 January 2023, where Complainant repeated his accusations that the Service Provider did nothing to protect him from fraudsters.

“I had built my crypto wallet over a few years and then I began trading on the forex market. A guy that I was trading with told me about a scheme (much like Cashavec scheme) where you can invest your crypto. They would do trading for you, and they will pay you back a dividend ... The website looked perfect ...

What happened is that as soon as I invested on their website where it shows you are earning money by doing the trading; but when it comes to the payouts, they started asking for more and more money. I gave them a little bit more, (it wasn't a little bit for me); then they were asking for more money. I was stuck in the cycle of giving them money before they would pay me back out.

And, before I knew it, they took everything away; what was in my crypto wallets. Basically, it all disappeared. It could be perceived I was being naïve, but once I started panicking that I was losing all my money, that the only way to get my money back seemed to be to pay what they were asking for ... Maybe I was a little bit naïve. I was scared when I lost that money and I just wanted to have my money back”.¹⁵

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

Apart from repeating their position as presented in their official reply to the Complaint, reference was made to the statement made by the Complainant in the first hearing where he said:

“The crypto wallet that I was paying into was with Crypto.com of this scammer. ... I know that he is still active probably still on Crypto.com”.¹⁶

¹⁴ P. 125 126

¹⁵ P. 144

¹⁶ *Ibid.*

The Service Provider refuted these allegations and stated:

“The wallet which he transferred funds to is an external wallet; not under the control of Crypto.com or one of our registered users from what we can see. This is supported by evidence that we filed with the Tribunal as document FS 5, where you can see that the transactions occurred between Crypto.com Master account to an external account not under our control.

As with all these complaints, it is important to note that there is no way to verify what the complainant himself has accessed to this third-party wallet to which he sent the Ethereum simply because the third-party wallet is not one that we provide and therefore we have no details of this cryptocurrency account.

One person can hold multiple accounts without any links between them. The registration or the KYC information is not held by Crypto.com simply because it is not a wallet provided by us.

On the balance of the foregoing, we would submit that the complainant authorised the transactions himself. All the transactions were carried out on his specific instructions. If a scam has occurred, which we have no evidence to verify or disprove, we would say that it occurred out of his gross negligence and after the fact that the complainant only contacted us after all the transactions had been completed and had occurred.

There is nothing that the service provider could do for the complainant in these circumstances.”¹⁷

Furthermore, the Service Provider explained that as resulting in the transcripts of the call of 13 February 2022,¹⁸ the Complainant was forced to observe a 24-hour period for transferring assets to a wallet address he had just whitelisted. These transactions were in fact executed on the 14 February 2022.

Cross-examination of the Service Provider was made by written questions and answers.¹⁹

¹⁷ P. 188

¹⁸ P. 185 – FS-4

¹⁹ P. 195 - 197

Neither the cross-examination of the Service Provider, nor the final submission produced new relevant information. The parties stuck to their well-defined positions. The Complainant expecting the Service Provider to have monitor systems to protect him from his own naivety and from fraudsters, arguing these are needed for Anti-Money Laundering and Countering of Finance of Terrorism apart from preventing fraud and scams. The Service Provider arguing that under their Class 3 VFAA licence they had no such obligation and the Terms and Conditions which the Complainant accepted made clear that he was responsible to take the necessary safeguards that he is expecting from the Service Provider.

In addition, the Service Provider concluded that:

“17. 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.

18. In addition, the contractual relationship between the Complainant and the Respondent is clearly set out in the Terms and Conditions which the Complainant expressly agreed to and the Terms and Conditions clearly provide that the Complainant had the responsibility, among others, to verify all transaction information prior to submitting it to the Respondent. Furthermore, and in any case, the facts of the case and the nature of cryptocurrency transactions are such as to raise no reasonable suspicions as to their legitimacy.”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

²⁰ P. 205

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

Observations & Conclusion

Summary of main aspects

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. 155

²⁶ P. 119

The Complainant made a transfer of his digital assets (ETH) 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 reimbursement from Foris DAX for the Service Provider's failure to prevent, stop or reverse the payment 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.

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

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

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 US\$ 15,000.

The Complainant expected the Service Provider to prevent or stop his transactions. He claimed that the Service Provider had an obligation to warn him of potential fraud.

The Arbiter considers that no adequate and sufficient evidence has however emerged to substantiate the claim that the Service Provider 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 himself had “whitelisted” the address giving the all clear signal for the transfer to be executed.
- The Complainant seems to have only contacted the Service Provider late on 21 February 2022 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 Use²⁹ (and as typically indicated on various other internet sites).³⁰

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.³¹

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 ...”*³²

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 Clause 7.2(b) of the *Crypto.com* App Terms & Conditions - P. 178

³⁰ E.G. <https://www.chargebackgurus.com/blog/chargebacks-more-volatile-complex-than-cryptocurrency>

³¹ Clause 3.1 and Clause 7.2(b) of the Terms and Conditions on the use of the *Crypto.com* App Services (P. 159; 168)

³² P. 168

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:³³

“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”*.³⁴ In the said formal complaint reference was also made to *“The Federal Trade Commission (FTC) Act, 15 U.S.C.”*,³⁵ 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

³³ P. 169

³⁴ P. 8; 11

³⁵ P. 8

consumer protection measures applicable to a financial institution falling under EU regulatory regimes.³⁶

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 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.³⁷

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

³⁶ 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).

³⁷ 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/>

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.³⁸

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.

³⁸ 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

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.

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