Before the Arbiter for Financial Services

Case ASF 194/2024

KO

('the Complainant')

vs

Foris DAX MT Limited

(Reg. No. C 88392)

('Foris' or 'the Service Provider')

Sitting of 30 May 2025

The Arbiter,

Having seen the Complaint made against Foris DAX MT Limited relating to its alleged failure to warn client that his transfer of USDT 15,736.31, Bitcoin (BTC) 1.4854976 and ETH 8.095[1] to a fraudulent platform has caused him a financial loss for which he is seeking compensation of €70,500[2] being the fiat currency transfers effected to finance the acquisition of the crypto assets transferred to fraudsters.

The Complaint[3]

In his Complaint Form to the Office of the Arbiter for Financial Services ('OAFS'), the Complainant submitted that he was a victim of a cybercrime perpetrated through *Crypto.com* whose misconduct allowed the fraudster operating through trading platform NIXSE to steal his money.

[1] Page (p.) 61
[2] P. 3
[3] P. 1- 6 with supporting documentation on P. 7 - 50.

He claims to have made 3 transfers totalling €70,500 from his bank accounts in France to his account with Crypto.com to invest as pressurised by NIXSE who had promised substantial profits from his investments. These transfers were made as follows:

Date	**Amount in EURO**	**Remitter bank**[4]	**Crypto assets bought**	
06.06.2023	5000	Belfius Bank Belgium	USDT	5180
27.06.2023	10000	‘’	USDT	10557.91
29.09.2023	55500	‘’	BTC	1.5
			ETH	8.2
TOTAL	**70500**			

In his complaint, it was also submitted that on 24 November 2023, Complainant requested withdrawal of €10,000 from his account with NIXSE but this was refused and, consequently, incurred a loss of €70,500 for which he seeks compensation from Service Provider as he maintains:

“*The bank’s duty of non-interference in the customer’s affairs ceases to apply when it is shown that a disputed transaction is tainted by an ‘apparent anomaly’, of a material or intellectual nature, which raises a risk of illegality. In such cases, the banker is required at the very least to question his customer and inform him of the potentially suspicious nature of the planned transaction.*

It is in this sense that any significant change in the usual operation of the bank account is an anomaly that must be identified by the banker (CA Agen, January 6, 2016, no. 14/00480).

[4] P. 81; 26

In view of the size of the transfers, the bank is subject to graduated measures of vigilance with regard to its customers, both before and during the relationship; this essentially involves collecting, retaining and declaring information relating to supposedly suspicious transactions. The banker may even refuse to carry out the requested order, as stipulated in article L. 561-8 of the Monetary and Financial Code."

One notes that in his complaint, the Complainant refers to Foris as 'Bank' and imputes to them certain obligations under the EU Directive PSD 2[5] that are applicable to banks but not applicable to VFA operators.

The Complainant, realising it was a scam, made a report to the relevant French Authorities.[6]

In his complaint, he presented extensive documentation of contracts and correspondence exchanged with NIXSE explaining the investment. However, as the Arbiter has no competence against NIXSE, this documentation is quite irrelevant to this complaint as Foris was not a party to such contracts and had no access to such knowledge at the time when the transfers complained of were being executed.

He maintained that Service Provider should have detected the irregularity of the transactions on his account and therefore held them responsible for his loss.

He claims that Foris should have protected him from sending his assets to the wallets controlled by the fraudsters and quoted various references to French law on this matter.[7]

Complainant denied he was guilty of negligence and explained:

'***a. No negligence on the part of the customer***

In law*, all banks are required to distinguish between two types of customers. Firstly, a person who is not aware of the risks, generally an individual, will be eligible for the bank's duty to warn. Then, a well-informed person, generally a*

[5] EU Directive 2015/2366 – Payment Services Directive commonly referred to as PSD 2.
[6] P. 30 – 33 and attachments.
[7] P. 10 - 12

professional, will be presumed to be aware of the risks associated with investment transactions.

In principle, the payer bears all losses caused by unauthorised payment transactions if these losses are the result of fraudulent conduct on his part, or if he has intentionally or through gross negligence failed to comply with the obligations set out in articles L. 133-16 and L. 133-17 of the French Monetary and Financial Code L.133-17 of the French Monetary and Financial Code.

<u>These obligations are</u>:

- *to take all reasonable measures to preserve the security of personalised security data, and*
- *informing the payment service provider without delay of cases of embezzlement and stopping fraudulent payments.*

However, the burden of proof of fraudulent conduct, intentional breach of duty or gross negligence on the part of the user lies with the payment service provider. Moreover, such proof cannot be deduced from the mere fact that the payment instrument or the personal data linked to it were actually used".[8]

Service Provider's reply

Having considered, in its entirety, the Service Provider's reply[9]

Where the Service Provider provided a summary of the events which preceded the Complainant's formal complaint and explained and submitted the following:

"Background

- *Foris DAX MT Limited (the "**Company**") offers the following services: a crypto custodial wallet (the "**Wallet**") and the purchase and sale of digital assets through the Wallet. Services are offered through the Crypto.com App (the "**App**"). The Wallet is only accessible through the App and the latter is only accessible via a mobile device.*

[8] P. 11
[9] P. 56 - 62 with attachments from p. 63 - 68

- *Our company additionally offers a single-purpose wallet (the "**Fiat Wallet**"), which allows customers to top up and withdraw fiat currencies from and to their personal bank account(s). This service is offered by the legal entity Foris MT Limited.*
- *Mr … (the "Complainant"), e-mail address ……. became a customer of Foris DAX MT Limited through the Cryto.com App and was approved to use the Wallet on 5 June 2023.*
- *The Company notes that in the submitted complaints file, (the Complainant's) representative has outlined the desired remedy as: (i) reimbursement for incurred financial losses."*[10]

The Service Provider then provided a timeline for the transactions of the Complainant's account with them. These included above listed inward transfers of Euro fiat currency collectively amounting to €70,500. These funds were then converted to crypto assets (USDT, BTC and ETH) and transferred to two external wallets on the instructions of the Complainant between 06 June 2023 and 06 October 2023.

The Service Provider concluded that:

"Based on our investigation, the Company has concluded that we are unable to honor the Complainant's refund request based on the fact that the reported transfers were made by (the Complainant) himself.

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

[10] P. 56

The Complainant is solely responsible for the security and authenticity of all instructions submitted through his Wallet as outlined in the Foris DAX MT Limited Terms of Use.

Please see the relevant section of the Terms of Use for your reference.

QUOTE

7.2 Digital Asset Transfers

…

(b) Crypto.com processes all Digital Asset Transfers according to the instructions received from you and does not guarantee the identity of any recipient. You should verify all transaction information prior to submitting instructions for a Digital Asset Transfer to Crypto.com as the Digital Asset Transfer may not be cancelled or reversed once processed by Crypto.com unless Crypto.com decides at its sole discretion that the transaction should be cancelled or reversed and is technically capable of such cancellation or reversal. You acknowledge that you are responsible for ensuring the accuracy of any instructions submitted to Crypto.com and that any errors may result in the irreversible loss of your Digital Asset.

…

UNQUOTE

In summary, it seems conceivable that the Complainant has been the victim of an alleged scam. However, due to the nature of the external wallet and the fact that it is not hosted or operated by Foris DAX MT, we can neither confirm nor deny this.

Whilst we fully empathize with (the Complainant) in this regard, it cannot be overlooked that he had willingly, transferred his virtual asset holdings from his Crypto.com Wallet to an external wallet address which he nominated.

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."[11]

Hearings

During the hearings, the Complainant failed to make presence and was represented by his French counsel.

This raised objections from the Service Providers who in the absence of possibility to cross-examine the evidence submitted by Complainant claimed that such evidence should not be considered.

The Arbiter ruled that in the absence of Complainant making himself available for cross-examination, he is taking a clear position that the payments and transfers complained of were executed with the full authority of the Complainant and the Service Provider will only be asked to defend themselves from the claim that through their monitoring systems they should have stopped the transfers to external wallets controlled by the fraudsters as there were clear signs of fraud.

Complainant's lawyers assented to such decision whilst Service Provider wished to register the following statement:

"***I would like to have a general statement in the note verbal of all these cases with regard to the fact that as agreed, the evidence of the complainant was not given; it was given by his representative, and the cross-examination was very limited.***

However, I do not want that to be an acceptance of all the other allegations being made by the complainant. So, I want to make it clear from the service provider's side that the absence of the complainant's testimony is not being taken as an acceptance of his allegations, but it is rather being dismissed and obviously it cannot be considered evidence because he is not available.

So, everything else is being dismissed because the only assumption and the only thing that Foris DAX has accepted is that there is the authorisation of the complainant and that has been accepted; but everything else is not being

[11] P. 61 - 62

accepted, that is, whatever the complainant said for which he has not been called in to testify."[12]

The Complainant's representative asserted:

"***So, we really want to make a point that the individuals involved in all the cases were indeed the ones who initiated the transfers to the Crypto.com platform. We do not dispute that the victims themselves initiated and authorised these transfers.***

Our primary concern today, what we want to point out to you is whether Crypto.com had a duty of prevention and vigilance.

And, so, it is important for us to tell you that we were not disputing about who initiated the transfers. We know that it's the victims themselves who authorised the transfers."[13]

It was established during the first hearing of 17 February 2025, that Complainant intends to open a complaint against his Belgian Bank to hold them responsible for not withholding the transfers he was making to his Crypto.com account.[14]

During the second hearing of 01 April 2025, the Service Provider submitted:

"***The complainant in this case became a user of the service provider on the 5th of June 2023 and, through a series of withdrawals which occurred between the 6th of June 2023 and the 6th of October 2023, he withdrew a total amount of roughly 15,736 USDT, 1.485 Bitcoin and 8.1 Etherium. These cryptocurrencies were withdrawn over a series of transactions to two wallet addresses in question, one for the USDT and the Ethereum amounts, the second for the total of the Bitcoin amounts being on different blockchains.***

Now, at the time, these transactions occurred Crypto.com did have transaction monitoring and continues to do so. The transaction monitoring carried out by Crypto.com, whether by itself or through its service providers, did not reveal any warnings or flags for the withdrawal addresses in question. None of the withdrawal addresses in question are operated by Crypto.com. We do not have

[12] P. 84
[13] P. 82
[14] P. 81

any information on them, but what we can say is that the transaction monitoring did not detect anything unusual with these transactions and on that basis, and taking also the concession by the complainant that these transactions are authorised by them, we would say that Crypto.com bears no responsibility for any of the results or consequences of the withdrawals which had occurred and carried out pursuant to the user's express instructions.

These are the submissions or the evidence of the service provider with regards to this case."[15]

Complainant's representatives declined to cross-examine the evidence of the Service Provider.

Final Submissions

In their final submissions, the parties basically repeated what had already emerged in the complaint, the reply and the hearing proceedings.

Having heard the parties

Having seen all the documents

Considers

In failing to give proper evidence before the Arbiter and denying the Service Provider their right for a proper cross-examination of the case made in his complaint, the Complainant has substantially prejudiced his case. As the identity of the beneficial owners of the external wallets recipients of the claimed fraudulent payments cannot be established, it was necessary to hear an emphatic negation from the Complainant that he himself was not a party to such wallets. Such emphatic negation was only forthcoming from the side of the Service Provider.

Applicable Regulatory Framework

Foris DAX was, at the time of the events leading to this complaint, the holder of a Class 3 VFAA licence granted by the Malta Financial Services Authority ('MFSA') under the Virtual Financial Assets Act, 2018 ('VFAA').

[15] P. 83 - 84

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

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

The Arbiter further notes that in the year 2020, the MFSA has also issued a *'harmonised baseline guidance on Technology Arrangements'*[16] 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 unknown external wallets.

  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

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

nature of the transactions 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.

- The Complainant seems to have only contacted the Service Provider on 22 November 2023, some 4 months after the last of the disputed transactions was already executed and finalised.[17]

  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).[18]

  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.

  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

[17] 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).
[18] 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 …".[19]

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.

In arriving at his decision, the Arbiter considered the following aspects:

i. AML/CFT Framework

Further to the Prevention of Money Laundering Act (Cap. 373) and Prevention of Money Laundering and Funding of Terrorism Regulations ('PMLFTR'), the Financial Intelligence Analysis Unit (FIAU) issued Implementing Procedures including on the *'Application of Anti-Money Laundering and Countering the Funding of Terrorism Obligations to the Virtual Financial Assets Sector'*.[20]

These are *'sector-specific Implementing Procedures [which] complement the Implementing Procedures – Part I [issued by FIAU] and are to be read in conjunction therewith'*.[21] Section 2.3 of these Implementing Procedures detail the monitoring and transaction records obligations of VFA licensed entities.

It is noted that the VFA Act, mainly imposes transaction monitoring obligations on the Service Provider for the proper execution of their duties for Anti Money Laundering ('AML') and Combating of Financing of Terrorism ('CFT') obligations in terms of the local AML and CFT legislative framework.

Failures of the Service Provider in respect of AML/CFT are not in the remit of the OAFS and should be addressed to the FIAU. In the course of these procedures, no such failure was indeed alleged. The Arbiter shall accordingly not consider compliance or otherwise with AML/CFT obligations in this case.

[19] P. 62
[20] https://fiaumalta.org/app/uploads/2020/09/20200918_IPsII_VFAs.pdf
[21] Page 6 of the FIAU's Implementing Procedures on the *'Application of Anti-Money Laundering and Countering the Funding of Terrorism Obligations to the Virtual Financial Assets Sector'*

ii. MiCA and the Travel Rule

As to the identification of the recipient of the funds, it is noted that MiCA[22] and Travel Rule[23] obligations which entered into force in 2025, and which give more protection to consumers by having more transparency of the owners of the recipient wallets were not applicable at the time of the events covered in this Complaint which largely happened in 2023. The Arbiter shall thus not consider the MiCA provisions and Travel Rule obligations for the purposes of this Complaint.

iii. Othis - Technical Note

A Technical Note (issued in 2025) with guidance on complaints related to pig butchering was recently published by the Arbiter.

In respect of VFA licensees the Technical Note states as follows:

> *"Virtual Financial Assets Service Providers (VASPs)*
>
> *VASPs should be aware that with the coming into force of Regulation (EU) 2023/1113 and the Travel Rule Guidelines[24] their obligation to have reliable records on the owners of external (unhosted) wallets increases exponentially as from 30 December 2024.*
>
> *Arguments that they have no means of knowing who are the owners of external wallets which have been whitelisted for payments by their client will lose their force. VASPs have been long encouraged by the Office of the Arbiter (in decisions dating back from 2022),[25] for the devise of enhanced mechanisms to mitigate the occurrence of customers falling victims to such scams.*

[22] EU Directive 2023/1114 on markets in crypto assets https://eur-lex.europa.eu/legal-content/EN/AUTO/?uri=celex:32023R1114

[23] EU Directive 2023/1113 https://eur-lex.europa.eu/legal-content/AUTO/?uri=CELEX:32023R1113&qid=1740401464257&rid=1 and EBA Guidelines on Travel Rule https://www.eba.europa.eu/sites/default/files/2024-07/6de6e9b9-0ed9-49cd-985d-c0834b5b4356/Travel%20Rule%20Guidelines.pdf

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

[25] Such as Case ASF 158/2021

Furthermore, in the Arbiter's decisions of recent months there is a recommendation that VASPs should enhance their on-boarding processes where retail customers are concerned warning them that custodial wallets may be used by scammers promoting get-rich-quick schemes as a route to empty the bank accounts of retail customers and disappear such funds in the complex web of blockchain anonymous transactions.[26]

***Compliance with such recommendations or lack thereof will be taken into consideration in future complaint adjudications**."*[27]

The Arbiter will not apply the provisions of the Technical Notes retroactively.

Hence, for the avoidance of any doubt, the said Technical Note is not applicable to the case in question.

iv. Duty of Care and Fiduciary Obligations

It is noted that Article 27 of the VFA Act states:

"27. (1) Licence holders shall act honestly, fairly and professionally and shall comply with the requirements laid down in this Act and any regulations made and rules issued thereunder, as well as with other legal and regulatory requirements as may be applicable.

***(2) A licence holder shall be subject to fiduciary obligations as established in the Civil Code (CAP 16) in so far as applicable**."*[28]

Article 1124A (1)(a) of the Civil Code (Chapter 16 of the Laws of Malta), in turn further provides the following:

"1124A. (1) ***Fiduciary obligations arise in virtue of law, contract, quasi-contract****, unilateral declarations including wills, trusts,* ***assumption of office or behaviour whenever a person*** *(the ''fiduciary'') –*

(a) ***owes a duty to protect the interests of another person and it shall be presumed that such an obligation where a fiduciary***

[26] Such as Case ASF 069/2024
[27] Emphasis added by the Arbiter
[28] Emphasis added by the Arbiter

acts in or occupies a position of trust is in favour of another person …"[29]

It is further to be pointed out that one of the High Level Principles outlined in Section 2, Title 1 *'General Scope and High Level Principles'* Chapter 3, Virtual Financial Assets Rules for VFA Service Providers of the VFA Rulebook, that applied to the Service Provider at the time of the disputed transactions in 2022, provides that:

"R3-1.2.1 VFA Service Providers shall act in an ethical manner taking into consideration the best interests of their clients and the integrity of Malta's financial system."

It is also noted that Legal Notice 357 of 2018, Virtual Financial Assets Regulations, 2018 issued under the VFA Act, furthermore, outlined various provisions relevant and applicable to the Service Provider at the time. Article 14 (1) and (7) of the said Regulations, in particular, which dealt with the *'Functions and duties of the subject person'* provided the following:

"14. (1) A subject person having the control of assets belonging to a client shall safeguard such assets and the interest of the client therein.

…

(7) The subject person shall make appropriate arrangements for the protection of clients' assets held under control and shall ensure that such assets are placed under adequate systems to safeguard such assets from damage, misappropriation or other loss and which permit the delivery of such assets only in accordance with the terms and conditions of the agreement entered into with the client."

The Arbiter is of the view that for the general fiduciary obligations to apply in the context of the VFA ACT, there must be something which is truly out of the ordinary and which should really act in a conspicuous manner as an out of norm transaction which triggers the application of such general fiduciary duties. No such out of norm event can be claimed during the short period of some four months when the funds were being transferred from Complainant's account

[29] Emphasis added by the Arbiter

with his Belgian Bank Belfius. Even the last payment for €55,500 was not abnormal for someone who wanted to invest in Bitcoin which at the time was trading at a price of around €25k per unit.

The Arbiter thus considers that the Service Provider did not breach, in terms of the provisions outlined in this decision, the duty of care and fiduciary obligations towards its customer, the Complainant, when considering the particular circumstances of this case.

Decision

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* existed at the time of the disputed transactions. An EU regulatory framework was only recently implemented effective for the first time in this field in 2025.[30]

Whilst this area of business had remained unregulated in certain jurisdictions, other jurisdictions, like Malta, chose to regulate this field in the meantime and subject it to a home-grown national regulatory regime. While such regimes 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

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

been regulated. In fact, the Arbiter notes that in his Complaint, the Complainant refers to provisions of the PSD 2,[31] as translated into French legislation which, whilst applying to Banks, are not applicable to VFA licensees.

The Arbiter notes that Complainant's representatives expressed intention to make similar claims for compensation from Belfius Bank on the basis that they had an obligation to intervene and stop Complainant from transferring his funds to a crypto exchange, given the much longer relationship between Complainant and his Bank permitting them to view in better context the abnormality of such payments.

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.[32]

The Arbiter sympathises with the Complainant for the ordeal he may have 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.

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

Alfred Mifsud
Arbiter for Financial Services

[31] EU Directive 2015 - 2366
[32] https://www.eiopa.europa.eu/document-library/othis-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

Information Note related to the Arbiter's decision

Right of Appeal

The Arbiter's Decision is legally binding on the parties, subject only to the right of an appeal regulated by article 27 of the Arbiter for Financial Services Act (Cap. 555) ('the Act') to the Court of Appeal (Inferior Jurisdiction), not later than twenty (20) days from the date of notification of the Decision or, in the event of a request for clarification or correction of the Decision requested in terms of article 26(4) of the Act, from the date of notification of such interpretation or clarification or correction as provided for under article 27(3) of the Act.

Any requests for clarification of the award or requests to correct any errors in computation or clerical or typographical or similar errors requested in terms of article 26(4) of the Act, are to be filed with the Arbiter, with a copy to the other party, within fifteen (15) days from notification of the Decision in terms of the said article.

In accordance with established practice, the Arbiter's Decision will be uploaded on the OAFS website on expiration of the period for appeal. Personal details of the Complainant(s) will be anonymised in terms of article 11(1)(f) of the Act.