

Before the Arbiter for Financial Services

Case ASF 038/2025

YV

(‘the Complainant’)

vs

Foris DAX MT Limited

(Reg. No. C88392)

(‘Foris’ or ‘the Service Provider’)

Sitting of 28 August 2025

The Arbiter,

Having seen the Complaint made against Foris DAX MT Limited relating to its alleged failure to warn client that her transfer of digital assets (which digital assets were funded by transfer of Euro currency from her Bank account to her account with Service Provider) to a fraudulent platform, has caused her a financial loss for which she is seeking compensation of €86,300¹.

The Complaint²

In her Complaint Form to the Office of the Arbiter for Financial Services (‘OAFS’), the Complainant submitted that she was a victim of a cybercrime perpetrated through *Crypto.com* whose misconduct allowed the fraudster operating an unidentified investment platform to steal her money. She stated that after registering for a wallet account on *Crypto.com* (brand name of the Service provider) she was contacted by alleged advisers offering Bitcoin investments with a promise of advantageous annuities. These made contact via email and Whatsapp all showing contact numbers starting +44, being a UK country code.

¹ P. 4

² P. 1 - 7 with supporting documentation on P. 8 - 60

She claims to have started with a minimum investment of €250 but this was followed by larger transfers from her account with Société Générale in France to her account with Crypto.com to invest as pressurised by fraudsters, as follows:

Date	Amount in EURO	Reference
20.09.2022	3,000	p. 23
14.12.2022	50,000	p. 20
21.02.2023	6,000	p. 21
03.03.2023	15,000	p. 21
06.04.2023	12,300	p. 18/19 show this payment was first made on 29.03.2023 and returned on 31.03.2023. It was made again on 03.04.2023 and returned on 05.04.2023. Then finally made on 06.04.2023.
TOTAL	86,300	Service Provider does not acknowledge receipt of last payment of 12,300 so that funds received in her Crypto account are acknowledged for €74,000.

In her Complaint, she explained that after making the payment for €50,000, she became suspicious and requested return of her investments. However, the fraudsters explained that for fake '*so-called synchronisation procedure*',³ she had to make the last 3 payments before her funds could be returned.

She filed a report with French Police on 21.03.2023⁴ and a bailiff report on 25.09.2023⁵.

She seeks compensation from Service Provider for her total loss of €86,300 even though Service Provider could account only for funds received in her account for €74,000.

³ P. 3

⁴ P. 29 - 31; not clear why she alleges to have made the last payment of €12,300 in three attempts (as shown in table above) after filing the police report. However, in the conversations in French with the fraudsters included in the bailiff's report (see next footnote), she makes reference to installation of Anydesk app which gives fraudsters access to her account to continue their fraud and her victimisation.

⁵ P. 33 - 60

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

She claims that Foris should have protected her from sending her assets to the wallets controlled by the fraudsters and quoted various references to French law on this matter.⁶

Complainant denied she was guilty of negligence and explained that she had no intention of transferring her money for purposes other than investment and Service Provider (whom she addresses as Bank/neobank) failed to note the unusual nature of the transfers.⁷ She then quotes various transaction monitoring obligations related to banks and finally concludes as follows:

“In this case, (Complainant) did not make any mistake. Indeed, she was quick to contact her adviser to obtain further information about her situation when she became aware that the entire procedure was fraudulent. In addition, (Complainant) did not disclose any personal data to third parties. Consequently, Service Provider must return customer’s funds as she has not committed any fault”.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:

1. “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.*

⁶ P. 10 - 13

⁷ P. 11

⁸ P. 12 - 13

⁹ P. 66 - 72 with attachments from p. 73 - 78

- *Our Company additionally offers a single-purpose wallet (the ‘**Cash Wallet**’) (formerly referred to as the Crypto.com Fiat (EUR) 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.*
- *(The Complainant), e-mail address xxxxx@gmail.com, became a customer of Foris DAX MT Limited through the Crypto.com App and was approved to use the Wallet on 6 September 2022.*
- *The Company notes that in the submitted complaints file, the Complainant’s representative has outlined her desired remedy as: (i) reimbursement for incurred financial loss.”¹⁰*

The Service Provider then provided a timeline for the transactions of the Complainant’s account with them. These included above listed 5 inward transfers of Euro fiat currency collectively amounting to €74,000.

These funds were then converted to crypto assets (Bitcoin - BTC) and transferred to four external wallets on the instructions of the Complainant between 22 September 2022 and 07 March 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 herself.

While we sympathize with the Complainant and recognize that she 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 wallets.

¹⁰ P. 66

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

The Complainant is solely responsible for the security and authenticity of all instructions submitted through her 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

6.2

Without prejudice to the foregoing and any other terms in these Terms, we assume that any and all instructions received from your Enabled Device have been made by the rightful owner. You are solely responsible and liable for keeping your enabled Device safe and maintaining adequate security and control of your login and authentication details (including, but not limited to, your username, and password), and shall likewise be solely responsible for any access to and use of the Crypto.com App and the Services through your Enabled Device, notwithstanding that such access and/or use may have been effected without your knowledge, authority or consent. We will not be liable to you for any loss or damage resulting from such access and/or use.

...

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 she had willingly transferred her virtual asset holdings from her Crypto.com Wallet to external wallet addresses which she 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 her French counsel.

This raised objections from the Service Provider 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 herself 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 need only 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 ruling whilst Service Provider wished to register the following statement:

¹¹ P. 71 - 72

“I would like to make a short statement on the absence of the complainant.

I contest the fact that the complainant is not present as it is a well-established principle at law that anyone who is initiating proceedings must actively participate in those proceedings. The fact that the complainant is not present, consequently, gives the regrettable status of the service provider that it is unable to effectively address and challenge the facts made in the complaint and the allegations also made in the complaint and, thereby, hindering Foris DAX the opportunity to protect and uphold its name and reputation.

The purpose of cross-examination is not only a contestation, but it is also evidence in itself. So, Foris DAX and I, as the representative, would like to make it amply clear that this is not an acceptable position, and it is being contested for all intents and purposes.

I cannot make a cross-examination, not even on the transaction documents. It is what it is. I cannot ask the lawyer anything.”¹²

The Arbiter explained that as Complainant has accepted that she had personally authorised the transfers subject of this Complaint, the issue of not being at fault because she did not disclose her secret credentials is irrelevant. The relevant issue is whether the Service Provider could or should have done anything, according to law and regulations, to identify the fraud and stop the payments in spite of their being fully authorised.

During the second hearing of 10 June 2025, the Service Provider submitted:

“The complainant became a client and user of the service provider on 6 September 2022.

The first transaction was on 21 September 2022.

The disputed transactions in question relate to withdrawals of bitcoin, a cryptocurrency which is purchased on Crypto.com App to four different wallet addresses. These wallet addresses are what we call non-custodial addresses which means that they are not services provided services from Crypto.com or as identified from data on the blockchain not provided by service providers of other companies in this sphere.

¹² P. 80 - 81

*From the evidence at hand, there is nothing to suggest that these transactions were anything but authorised by the complainant herself. There's no suggestion that these transactions were not authorised by her yet completed to her requests in each and every case. At the time of the withdrawals, none of the address wallets in question or the wallet addresses in question were subject to any warnings from our own internal investigations or any third-party transaction monitoring tools that we use. And as such, we have no responsibility for the withdrawals in so far that they seem to have been pursuant to user's instructions. There was nothing in our own controls as well as the controls of our third-party employed tools to indicate that there was any malicious or scam activity involved in these cases at the time these happened, we were not communicated with or brought to the attention of the complainant's concerns with these transactions until after these transactions had already been completed. And, therefore, insofar that the transactions have been completed to the full satisfaction of what we were asked to execute on behalf of the complainant, we would say that we have no responsibility with regards to any of these transactions."*¹³

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 her Complaint, the Complainant has substantially prejudiced her 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 she herself was not a party to

¹³ P. 93 - 94

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 VFSA licence granted by the Malta Financial Services Authority ('MFSA') under the Virtual Financial Assets Act, 2018 ('VFSA').

Apart from the relevant provisions under the VFSA, 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 VFSA 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*'¹⁴ 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 herself transferred to an external wallet from her crypto account. At no stage has the Complainant raised any doubt as to her having authenticated the transactions personally.

¹⁴ Guidance 1.1.2, Title 1, '*Scope and Application*' of the '*Guidance on Technology Arrangements, ICT and Security Risk Management, and Outsourcing Arrangements*'.

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 her 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 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 her crypto.
- The Complainant seems to have only contacted the Service Provider on 15 November 2023¹⁵ some 8 months after the last of the disputed transactions was already executed and finalised.¹⁶

Once finalised, the crypto cannot be cancelled or reversed as specified in the Service Provider's Terms and Conditions of Use (and as typically indicated on various other internet sites).¹⁷

Once a transaction is complete and, accordingly, is not in a pending state, the crypto transaction cannot be cancelled or reversed by the Service

¹⁵ P. 15

¹⁶ 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).

¹⁷ E.G. <https://www.chargebackgurus.com/blog/chargebacks-more-volatile-complex-than-cryptocurrency>

Provider as provided for and warned in the Terms and Conditions of Foris DAX.

As indicated by the Service Provider, Clause 7.2(b) of its Terms and Conditions regarding the use of the Crypto.com App Services specifies that:

*“Crypto.com processes all Digital Asset Transfers according to the Instructions received from you and does not guarantee the identity of any recipient. You should verify all transaction information prior to submitting Instructions for a Digital Asset Transfer to Crypto.com as the Digital Asset Transfer may not be cancelled or reversed once processed ...”.*¹⁸

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*’.¹⁹

These are ‘*sector-specific Implementing Procedures [which] complement the Implementing Procedures – Part I [issued by FIAU] and are to be read in conjunction therewith*’.²⁰ 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

¹⁸ P. 71 - 72

¹⁹ https://fiaumalta.org/app/uploads/2020/09/20200918_IPsII_VFAs.pdf

²⁰ 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*’

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.

ii. MiCA and the Travel Rule

As to the identification of the recipient of the funds, it is noted that MiCA²¹ and Travel Rule²² 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. Other - 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 Guidelines²³ their obligation to have reliable records on the owners of external (unhosted) wallets increases exponentially as from 30 December 2024.

²¹EU Directive 2023/1114 on markets in crypto assets <https://eur-lex.europa.eu/legal-content/EN/AUTO/?uri=celex:32023R1114>

²² 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>

²³ *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>

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),²⁴ for the devise of enhanced mechanisms to mitigate the occurrence of customers falling victims to such scams.

Furthermore, in the Arbiter's decisions of recent months there is a recommendation that VASPs should enhance their onboarding 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.²⁵

Compliance with such recommendations or lack thereof will be taken into consideration in future complaint adjudications.²⁶

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.²⁷

²⁴ Such as Case ASF 158/2021

²⁵ Such as Case ASF 069/2024

²⁶ Emphasis added by the Arbiter

²⁷ Emphasis added by the Arbiter

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 acts in or occupies a position of trust is in favour of another person; ...”**.²⁸*

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

²⁸ Emphasis added by the Arbiter

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 six months when the fraudulent transfers were happening in relatively consistent quantity values in funds transferred from Complainant's account with her French Bank.

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 is 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 2025.²⁹

²⁹ 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/>

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 been regulated.

In fact, the Arbiter notes that in her Complaint, the Complainant refers to provisions of the PSD2,³⁰ as translated into French legislation, which whilst applying to Banks are not applicable to VFA licensees. She also often wrongly addresses Foris as a bank/neobank which clearly they are not.

The Arbiter was not informed whether any similar claims for compensation was made on Complaint's French Bank on the basis that they had an obligation to intervene and stop Complainant from transferring her funds to a crypto exchange, given the much longer relationship between Complainant and her Bank permitting them to view in better context the claimed abnormality of such payments. The Complainant's representative merely informed that matter was referred to a mediator following their notice to the French bank.³¹

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 she may have suffered as a victim of a scam but, in the particular circumstances of this case,

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

³⁰ EU Directive 2015 - 2366

³¹ P. 80

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

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

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.