Before the Arbiter for Financial Services

Case ASF 055/2025

SK

('the Complainant')

vs

Foris DAX MT Limited

(Reg. No. C88392)

('Foris' or 'the Service Provider')

Sitting of 28 November 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 digital assets (which digital assets were funded by transfer of Euro currency from his account with Société Générale in France to his crypto account with Service Provider) to a fraudulent platform, has caused him a financial loss for which he is seeking compensation of €34,000.[1]

The Complaint[2]

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 by a fraudulent investment platform NIXSE.com through *Crypto.com* whose

[1] Pages (p.). 3 - 4

[2] P. 1 - 7 with supporting documentation on P. 8 - 50.

misconduct allowed the fraudster operating the fraudulent platform to steal his money.

He stated that following his request for investment information on www.zoneeducation.fr, he was contacted by traders from NIXSE who guided him to make investments in digital assets promising strong returns.

In his complaint, he presented extensive documentation of contracts and correspondence exchanged with NIXSE explaining the investment.[3] 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.

In March 2024, assisted by the scammers, Complainant opened an account with Crypto.com (brand name of the Service Provider) and started funding such account with following Euro transfer from his bank account with Société Générale in France as follows:

Date	Amount in EURO	Reference
06.03.2024	10,000	p. 49
08.03.2024	7,500	p. 50
11.03.2024	5,000	p. 48
23.04.2024	3,000	p. 46
25.04.2024	4,500	p. 47
06.09.2024	2,000	p. 45
09.09.2024	2,000	p. 44
TOTAL	**34,000**	

He seeks compensation from Service Provider for his total loss of €34,000.

He maintained that Service Provider should have detected the irregularity of the transactions on his account and should, at the very least, have questioned him and informed him of the potential suspicious nature of the transactions.[4]

[3] P. 16 - 43
[4] P. 10

It was claimed that Foris should have protected Complainant from sending his assets to the wallets controlled by the fraudsters and quoted various references to French law on this matter.[5]

Complainant denied he was guilty of negligence and explained that he had no intention of transferring his money for purposes other than investment and Service Provider (whom he addresses as Bank/neobank) failed to note the unusual nature of the transfers.[6] He then quotes various transaction monitoring obligations related to banks and finally concludes as follows:

> *"In this case, (Complainant) made no mistake. Moreover, he did not disclose any personal data to third parties. Consequently, (Service Provider) must return the funds to the client as he committed no fault".*[7]

Service Provider's reply

Having considered in its entirety, the Service Provider's reply[8]

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.*

   - *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.*

[5] P. 10 -12
[6] P. ibid
[7] P. 11
[8] P. 57 - 67 with attachments from p. 68 - 85.

- *(The Complainant), e-mail address xxxx@yahoo.fr, became a customer of Foris DAX MT Limited through the Crypto.com App and was approved to use the Wallet on 5 March 2024.*
- *The Company notes that in the submitted complaints file, the Complainant's representative has outlined his desired remedy as: (i) reimbursement for incurred financial losses*."[9]

The Service Provider then provided a timeline for the transactions of the Complainant's account with them. These included above listed 7 inward transfers of Euro fiat currency collectively amounting to €34,000, as well as two other payments for €600 not included in the complaint.[10]

These funds were then converted to crypto assets (USDT) and the transferred through 17 transactions totalling USDT 36502.68 to external wallets ending with reference … 37C54 and … fcBc8.[11]

"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 wallets.*

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 his Wallet as outlined in the Foris DAX MT Limited Terms of Use.

[9] P. 57
[10] P. 57a €100 on 07.03.2024 and €500 on 08.03.2024
[11] P. 65

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 he had willingly, transferred his virtual asset holdings from his Crypto.com Wallet to external wallet addresses 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."[12]

Hearings

During the hearings the Complainant failed to make presence and was represented by his French counsel who largely restated the contents of the filed complaint.

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 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 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:

"On behalf of the service provider, I contest the fact that the complainant is absent.

[12] P. 65 - 66

I respectfully submit that the presence of the complainant is essential especially when the complainant himself triggered this process of arbitration.

The presence of the complainant is not only essential for cross-examination, but his testimony forms a substantial part of the evidence, and this is crucial in ensuring that what is being said in the complaint is also what the complainant wishes to say.

For the service provider, the cross-examination is not a mere formality but is a basic principle of law that tests the truth and credibility of the complainant and also provides information to the Arbiter on the negligence or otherwise of the complainant himself.

However, without this testimony, questions relating to the negligence or nature of the transaction cannot be understood or properly evidenced.

Therefore, any contributory factors can neither be assessed.

Denial of this opportunity to the service provided can prejudice its defence and, therefore, the service provider contests this absence for all intents and purposes."[13]

The Arbiter explained that as Complainant has accepted that he had personally authorised the transfers subject of this complaint,[14] the issue of not being at fault because he did not disclose his secret credentials is irrelevant. The relevant issue is whether the Service Provider could or should have anything, according to law and regulations, to identify the fraud and stop the payments in spite of their being fully authorised.

At the hearing, the Arbiter requested the Complainant's representative to file a translated copy of the fraud report made to the French Authorities and of the formal claim made against Société Générale.[15]

During the second hearing of 22 September 2025 (where complainant again failed to make presence), the Arbiter pointed out that the documents (translated) requested in the first hearing of June 2025 were not submitted by

[13] P. 88 - 89
[14] P. 86
[15] P. 89

the Complainant. Asked whether there were any developments about the claim on Société Générale, Complainant's legal representative had no information.

On 10 October 2025, alongside their final submissions (see below) Complainant's legal representative submitted a copy of the claim sent to Société Générale.[16]

It is strange that this claim is dated 18 December 2025 and that it includes claims related to the fraud payments extraneous to this complaint so that the total loss of Complainant is reported at €136,500, which includes the payments of €34,000 subject matter of this complaint. No indication was given as to the feedback, if any, received from the French Bank.

The Service Provider submitted the evidence of Ms Pema Fung who stated:

"Without repeating in detail what has already been filed in the service provider's reply, I would just like to highlight that a number of transactions occurred between the 8th of March and 9th of September 2024. In total, 17 withdrawals were made from the complainant's account totalling 36,502.68 USDT.

These were made to two external wallets. As agreed by Ms. Roskash in the first hearing, these transactions, the withdrawals, were all initiated or executed under the full authority and apparent consent of the complainant using his valid credentials in his account.

As the nature of the external wallets to which they were made were not operated, maintained, or controlled by the service provider, they accordingly fall outside of the scope of our service duties.

We would also like to highlight the fact that upon signing up for the complainant's Crypto.com account, he expressly agreed by ticking a box to agree to our terms and conditions, which clearly state that he, as the account holder, bears all responsibility for transactions executed using his credentials, including ones that they personally authorised, or, in other cases, where they have given authorisation to others to make these transactions through their account.

[16] P. 97 - 99

The service provider would also like to highlight that at the time of the transfers, under the question in this complaint, the service provider had no knowledge or indication that the receiving wallets were associated with any fraudulent activity.

Nor had any reports or alerts been generated to us in this regard.

We would also like to highlight that there was no information available at the time of the transactions to the service provider that gave rise to any reasonable or any suspicion of fraud which had necessitated action of the service provider under any of its general fiduciary obligations as contemplated under the applications provided.

Finally, the service provider would like to highlight the warnings that the complainant would have received during the whitelisting of the withdrawal address, as well as with each withdrawal he made to these external accounts.

He would have been warned that before being able to whitelist any address, he would have to have ticked that he trusted this address after being warned not to make any transfers to any investment platform promising unrealistically high returns, a person he does not know well, or any other source he was unsure of.

Once again, after this wallet was whitelisted before any and each withdrawal could be made, another pop-up would have appeared before a wallet withdrawal could be completed, also warning him of similar warnings and addressing him to another website, which would have taught him more about scams.

He would have had to click the button Confirm and Withdraw before any withdrawal could be made."[17]

Complainant's representative did not cross-examine the evidence.

Service Provider requested Arbiter's consent, which was given, to attach with their final submissions copies of the warnings given to Complainant every time he made a transfer to the external wallet and when originally the external wallet had been whitelisted by the Complainant.

[17] P. 90 - 92

Final Submissions

In their final submissions, the parties basically repeated what had already emerged in the complaint, the reply and the hearing proceedings. No additional documents were submitted by Foris regarding warnings given to clients every time they whitelist a wallet address and before each transfer is effected to an external wallet.

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 was 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').

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'*[18] applicable to its licence holders (including under the Virtual Financial Assets) titled *'Guidance on Technology Arrangements, ICT and Security Risk Management, and Outsourcing Arrangements'* ('the Guidance').

Further Considerations

Having considered the particular circumstances of the case including the submissions made and evidence provided, the Arbiter considers that there is no sufficient and adequate basis on which he can uphold the Complainant's request for the reimbursement by the Service Provider of the sum the Complainant himself transferred to an external wallet from his crypto account.

At no stage has the Complainant raised any doubt as to his having authenticated the transactions personally.

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

- The Complaint involves a series of payments made by the Complainant from his account held with Foris DAX to an unknown external wallet.

  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.

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

- 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 18 December 2024,[19] more than 3 months after the last of the disputed transactions was already executed and finalised.[20]

  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).[21]

  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.

  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. <u>AML/CFT Framework</u>

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*

[19] P. 8
[20] 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).
[21] E.G. https://www.chargebackgurus.com/blog/chargebacks-more-volatile-complex-than-cryptocurrency

Funding of Terrorism Obligations to the Virtual Financial Assets Sector'.[22] These are *'sector-specific Implementing Procedures [which] complement the Implementing Procedures – Part I [issued by FIAU] and are to be read in conjunction therewith'*.[23] 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.

ii. MiCA and the Travel Rule

As to the identification of the recipient of the funds, it is noted that MiCA[24] and Travel Rule[25] 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 happened in 2024. 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:

[22] https://fiaumalta.org/app/uploads/2020/09/20200918_IPsII_VFAs.pdf
[23] 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'*
[24] EU Directive 2023/1114 on markets in crypto assets https://eur-lex.europa.eu/legal-content/EN/AUTO/?uri=celex:32023R1114
[25] 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

"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[26] 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),[27] 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 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.[28]

***Compliance with such recommendations or lack thereof will be taken into consideration in future complaint adjudications**."[29]*

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:

[26] *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

[27] Such as Case ASF 158/2021

[28] Such as Case ASF 069/2024

[29] Emphasis added by the Arbiter

"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**."*[30]

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****;…"*[31]

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:

[30] Emphasis added by the Arbiter
[31] Emphasis added by the Arbiter

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

The Arbiter when considering the particular circumstances of this case, 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.

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.[32]

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 his complaint the Complaint refers to provisions of the PSD 2,[33] as translated into French legislation, which whilst applying to Banks are not applicable to VFA licensees. He also often wrongly addresses Foris as a bank/neo bank, which clearly, they are not.

The Arbiter was informed that 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 his funds to a crypto exchange, given the much longer relationship between Complainant and his Bank permitting them to view in better context the claimed 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

[32] 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/

[33] EU Directive 2015 - 2366

sectors of the financial services industry. EU regulatory bodies have issued various warnings to this effect over the past years.[34]

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.

However, the Arbiter warns that for new complaints registered after September 2025, in cases where the Complainants fail to attend hearings to defend their complaint without valid reasons, they will be obliged to settle the fees of the respondent service providers.

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

[34] 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

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.