Before the Arbiter for Financial Services

Case ASF 071/2025

AL

('the Complainant')

vs

Foris DAX MT Limited

(Reg. No. C 88392)

('Foris' or 'Service Provider')

Sitting of 6 February 2026

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 bank account with CIC LE TOUQUET to his account with Service Provider) to a fraudulent platform, has caused him a financial loss for which he is seeking compensation of €226,107.79.[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 person who called himself Raymond Lefort representative of NIXSE investment platform.

In his complaint, he presented extensive evidence of contracts and exchanges with various representatives of NIXSE related to investments. However, as the

[1] Page (p.) 4

[2] P. 1 - 7 with supporting documentation on P. 8 - 55.

Arbiter has no competence against NIXSE, whoever they may be, this documentation is quite irrelevant to this complaint as Foris was not a party to such knowledge and had no access to such knowledge at the time when the transfers complained of were being executed.

He claims that in total, he invested €226,107.79 through 15 transactions as shown in the Table below which were credited to his account with the Service Provider that was opened on 16.01.2024.

Sequence Number	**Date**	**Amount in EURO**	**Received by Service Provider**
1	19.01.2024	7,000	p. 63
2	22.01.2024	3,000	p. 63
3	02.02.2024	15,000	p. 64
4	14.02.2024	3,225	p. 65
5	15.02.2024	2,500	p. 66
6	22.02.2024	1,000	p. 67
7	23.02.2024	61,000	p. 68
8	28.03.2024	25,000	p. 70
9	03.04.2024	9,500	p. 72
10	17.04.2024	12,500	p. 73
11	13.05.2024	12,500	p. 74
12	29.05.2024	18,758	p. 75
13	05.06.2024	5,000	p. 77
14	13.06.2024	35,000	p. 78
	Sub-total	210,983.00	
15	14.06.2024	15,124.79	Not acknowledged
As per complaint	**Total**	**226,107.79**	

As can be seen from the above Table, there was a payment, No. 15, which Foris claim they never received and for which the Complainant could not provide satisfactory evidence that it was sent via his account with Foris (Crypto.com).

This payment is shown in folio 53 attached to the complaint but this is not sufficient evidence to prove it was actually sent to Foris. In the absence of provision of evidence about payment No. 15, the Arbiter decided that the amount of compensation to be considered in this complaint is for payments No. 1 to No. 14 acknowledged by Foris amounting to €210,983.

It needs to be mentioned that in the evidence submitted regarding a claim made on his home bank CIC LE TOUQUET, there is mentioned a further four payments amounting to €26,379 effected between 24.06.2024 and 12.07.2024 (after the payments listed in the Table above) so that the amount of the claim on the home bank increases to €245,485.79.[3]

There is a difference between the Table total plus the additional four payments and the amount claimed on the home bank and this could be related to an element of recoveries (€6,500).[4]

Be as it may, the amount of compensation was restated at €210,893 as above explained

It appears that the fraud was only reported to the French Authorities on 29.08.2025.[5] The formal claim against Foris was sent on 24.10.2024.[6]

From the Reply of Foris referred to hereunder, it results that each of these funds transfers were immediately converted to crypto assets and transferred to four external wallets so that by the end of the process, the Complainant had transferred to external fraudulent wallets USDT 202,167.33 between 25.01.2024 and 13.06.2024.[7]

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

[3] P. 144
[4] P. 135
[5] P. 132 - 140
[6] P. 8
[7] P. 79

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.[8]

Complainant denied he was guilty of negligence and explained that he had no intention of transferring his money for purposes other than investment and the Service Provider (whom he at times refers to as a bank) failed to note the unusual nature of the transfers.[9] He then quotes various transaction monitoring obligations related to banks and finally concludes as follows:

> *"In this case, (Complainant) made no mistake. He did not disclose any personal data to third parties. Consequently, our client's platform, CRYPTO, must return the funds to the client, as the latter committed no fault."*[10]

Service Provider's reply

Having considered in its entirety the Service Provider's reply,[11]

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.*

[8] P. 10 - 13
[9] *Ibid.*
[10] P. 12
[11] P. 62 - 80 with attachments from p. 81 - 124.

- *(The Complainant's), e-mail address xxxxx@wanadoo.fr, became a customer of Foris DAX MT Limited through the Crypto.com App and was approved to use the Wallet on 16 January 2024.*
- *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*.'[12]

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. These funds were then converted to crypto assets and transferred out to four external wallets as above referred to.

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 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.

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

QUOTE

[12] P. 62

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 the Company, 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.'[13]

Hearings

For the first hearing on 29 September 2025, the Complainant failed to make presence and was represented by his 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 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 and confirmed that all payments were made with full authority of the Complainant.[14]

The Arbiter explained that as Complainant has accepted that he had personally authorised the transfers subject of this complaint, 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 done anything, according

[13] P. 79 - 80
[14] P. 127

to law and regulations, to identify the fraud and stop the payments in spite of their being fully authorised.[15]

At the hearing, the Arbiter requested the Complainant's representative to file a copy of the fraud report made to the French Authorities and to inform whether a complaint was filed against his home bank.

The Arbiter also requested the Service Provider to submit copies of KYC documents at onboarding stage and any KYC related exchanges with Complainant during the course of the payments.

A copy of the report to French Authorities was sent following the first hearing.[16]

A copy of the claim against his home bank was sent also after the hearing.[17] This was dated 23.10.2025 but was attached to an email from Complainant's lawyer dated 10.10.2025. There results lack of clarity about the date of such claim on the home bank but it was evident that this was only filed after the first hearing that was held on 29.09.2025.

A second hearing was held 24 November 2025 for the evidence of the Service Provider. The Complainant was again not present for the second hearing and was only represented by his legal counsel, Samantha Roskach.

The Service Provider then proceeded with their evidence through Pema Fung and stated:

'The complainant became a client and user of the service provider on 16 January 2024, and the disputed transactions in question, which I won't repeat here, purchased on the Crypto.com app and sent to four different, external wallets between the 25 January and 13 June 2024.

These wallets are what we call non-custodial addresses, which means they are not serviced by Crypto.com or identified from data on the blockchain. They are not provided by service providers of similar companies.

[15] P. 129
[16] P. 132 - 140
[17] P. 142 - 148

From the evidence at hand, the agreement of the complainant, and the agreement of the complainant's legal representatives, these transactions were fully authorised by the complainant.

At the time of the withdrawals, it is important to highlight that none of the address wallets in question were subject to any warnings from our own internal investigations or any third-party transaction monitoring tools that we use.

As such, the service provider submits that we have no responsibility for the withdrawals, insofar as they seem to have been made pursuant to the complainant's instructions.

The service provider would also like to highlight the warnings that the complainant would have received during the transactions.

In the course of the complainant's disputed transactions, the service provider had provided numerous warnings regarding withdrawals to the external wallets.

The first of these warnings appears when a user adds a new withdrawal address to the Crypto.com app, which is called Whitelisting, and takes the form of a full-screen pop-up.

A similar warning appears again at the time of each withdrawal whether or not the withdrawal address is newly whitelisted or has been used before.

Both pop-up warnings specifically warn the complainant against scams and to not whitelist or withdraw digital assets to investment platforms touting unrealistically high returns, to people the complainant did not know well, and to any source the complainant did not have complete confidence in.

In respect of the warnings displayed during the withdrawals, the complainant is further warned that the withdrawal is irreversible.

The complainant was also encouraged to learn more about safety and protection from scams by clicking the link 'Learn More'. This link would take the users to a regularly updated Crypto.com Help Center page titled, 'Avoiding Digital Currency Scams'.

Upon the complainant confirming that they had read the scam warning by clicking on the Confirm and Withdraw button on the pop-up warning, the complainant confirmed that they accepted the risks involved and took full responsibility for withdrawals to the external wallets specifically agreeing to and acknowledging that the withdrawals were irreversible and that the service provider would not be liable for assets sent to external wallets.

In spite of the numerous warnings mentioned above, the complainant proceeded to make the withdrawals to the external wallets. It can be seen that the complainant either negligently disregarded the warnings or was, otherwise unaffected by them.

It is noted that the screenshots of these warnings have not yet been provided in the service provider's reply. Should Mr Arbiter require this evidence, we will be happy to include it in our final note of submissions with his permission.

Lastly, I would like to stress that there is nothing in our controls or external third-party employed tools that indicated any malicious activities or scams were involved in these cases at the time when they happened.

Nor was there any communication brought to the attention by the complainant regarding these transactions until these transactions had all been completed.

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 regard to these transactions.

I can confirm that we do not have any affiliation with NIXSE.'[18]

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

The Arbiter demanded that Foris submit the documentation he had asked for in the first hearing regarding KYC documentation of Complainant at onboarding stage[19] and any exchanges with him during the course of the payments subject of this complaint. He also asked formal submission of warnings given to Complainant referred to in Fung's evidence.[20]

[18] P. 151 - 153
[19] Received later, p. 163
[20] Received later, p. 159 - 162

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 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'*[21] 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 at no stage has the Complainant raised any doubt as to his having authenticated the transactions personally.

The Arbiter further considers 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 **except as deliberated hereunder under Fiduciary Duty obligations**, 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 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

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

'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 well after the last of the disputed transactions was already executed and finalised.[22]

  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).[23]

  Once a transaction is complete, and accordingly is not in a pending state, the crypto transaction cannot be cancelled or reversed by the Service Provider as provided for and warned in the Terms and Conditions of Foris DAX.

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

  'Crypto.com processes all Digital Asset Transfers according to the Instructions received from you and does not guarantee the identity of any recipient. You should verify all transaction information prior to submitting Instructions for a Digital Asset Transfer to Crypto.com as the Digital Asset Transfer may not be cancelled or reversed once processed …'.[24]

  Based on the facts presented during the case, the Arbiter could not conclude that, **except as treated hereunder under the Fiduciary Duty obligations**, 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:

[22] 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).
[23] E.G. https://www.chargebackgurus.com/blog/chargebacks-more-volatile-complex-than-cryptocurrency
[24] P. 80

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'*.

These are *'sector-specific Implementing Procedures [which] complement the Implementing Procedures – Part I [issued by FIAU] and are to be read in conjunction therewith'*.[25] 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. 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[26] and Travel Rule[27] 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 2023. The Arbiter shall thus not consider the MiCA provisions and Travel Rule obligations for the purposes of this Complaint.

[25] 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'*

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

[27] 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

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 Guidelines[28] 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),[29] 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.[30]*
>
> ***Compliance with such recommendations or lack thereof will be taken into consideration in future complaint adjudications**."[31]*

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

[28] *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

[29] Such as Case ASF 158/2021

[30] Such as Case ASF 069/2024

[31] Emphasis added by the Arbiter

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**."*[32]

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**; …".*[33]

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."*

[32] Emphasis added by the Arbiter
[33] Emphasis added by the Arbiter

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.

In the particular circumstances of this case, there is an event which is out of the ordinary to a degree which should have triggered the application of the fiduciary duties of the Service Provider, in particular:

1. In the AML document submitted[34] Complainant had indicated that he planned annual transactions for a value in the range €20,001 – €60,000 and an annual income in the range of €80,001 – €100,000.
2. As explained in the Table quoted above, the first 6 payments in the space of 33 days had cumulatively already reached €31,725. The 7th payment for €61,000 was transferred 1 day later taking the cumulative amount of payments to €92,725 well above the upper range of €60,000 indicated in the KYC document.

[34] P. 163

Furthermore, just one month later, the 8th payment for €25,000 was effected and this further pushed the cumulative number of payments to €117,725, basically double the upper annual range in the space of 10 weeks.

3. The Arbiter believes that at that point, on 28 March 2024, the pattern of payments compared to the KYC declaration should have triggered a few questions which the Service Provider failed to make.

4. Another 6 payments (nos. 9 to 14) for cumulative value of €93,258 bringing total cumulative payments to €210,983 in less than 5 months further accentuated the degree of the obligation to trigger questions which the Service Providers failed to make. Compared to an annual income higher range of €100,000 and annual turnover higher range of €60,000, there was a clear case to pause payments and ask questions to Complainant the answers to which could have generated suspicion of fraud.

For sake of clarity, the Arbiter explains that whilst he is not the competent authority to investigate breaches related to AML/CFT obligations, as earlier explained in this decision, he is competent to investigate whether in the process of performing such obligations, the Service Provider failed in its fiduciary duty to warn its customers of reasonable suspicion of fraud/scams emerging in the process of conducting its regulatory duties.

The Arbiter, when considering the particular circumstances of this case, considers that the Service Provider breached the duty of care and fiduciary obligations towards its customer, the Complainant. For this purpose, a copy of this decision is being sent to the Malta Financial Services Authority (Malta Regulator of CASPs) for their consideration of any regulatory action they may consider appropriate.

Decision

It is probable 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.

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.[35]

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,[36] as translated into French legislation, which whilst applying to Banks are not applicable to VFA licensees. He also at times wrongly addresses Foris as a bank which clearly, they are not.

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.[37]

In deciding what compensation, if any, would be appropriate in the particular circumstances of this case, the Arbiter has to consider whether the breach of fiduciary duty as above explained was the cause of the loss suffered by the

[35] Provisional agreement has been reached on the EU's Markets in Crypto-Assets Regulation (MiCA) only in June 2022 - https://www.consilium.europa.eu/en/press/press-releases/2022/06/30/digital-finance-agreement-reached-on-european-crypto-assets-regulation-mica/
MiCA entered into force in 2025 – https://www.financemagnates.com/cryptocurrency/can-mica-take-europe-to-the-crypto-promised-land/
[36] EU Directive 2015 - 2366
[37] 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

Complainant and whether there are any other factors which are more dominant contributors to such loss.

The Arbiter considers that there could be other dominant causes for this loss, namely:

1. The Complainant's gross negligence and greed in making investments expecting quick high returns without taking any advice or precautions.

2. The obligation of the home bank to spot the fraud and issue timely warning to Complainant.

The obligations of fiduciary duty and transaction monitoring apply more forcefully to licensed banks than they apply to CASPs/VFA agents. Banks have a much longer relationship with their clients, and they have the data to spot unusual transactions and suspect fraud. On the other hand, customer's relationship with a VFA is short without much historical data to enable early spotting of unusual patterns of payments.

Banks can only avoid, under the provisions of PSD 2, to reimburse fraud payments even if authenticated and authorised by their client, if the client has shown gross negligence in the process.

In terms of preamble 71 of the said PSD2,[38] the PSU (Complainant) shall be responsible for payment of any unauthorised payment transaction only up to a limit of €50, unless the PSU has acted fraudulently or with gross negligence.

[38] Preamble 71 of PSD 2 (**DIRECTIVE (EU) 2015/2366)** states**:**
In the case of an unauthorised payment transaction, the payment service provider should immediately refund the amount of that transaction to the payer. However, where there is a high suspicion of an unauthorised transaction resulting from fraudulent behaviour by the payment service user and where that suspicion is based on objective grounds which are communicated to the relevant national authority, the payment service provider should be able to conduct, within a reasonable time, an investigation before refunding the payer. In order to protect the payer from any disadvantages, the credit value date of the refund should not be later than the date when the amount has been debited. In order to provide an incentive for the payment service user to notify, without undue delay, the payment service provider of any theft or loss of a payment instrument and thus to reduce the risk of unauthorised payment transactions, the user should be liable only for a very limited amount**, unless the payment service user has acted fraudulently or with gross negligence**. In that context, an amount of EUR 50 seems to be adequate in order to ensure a harmonised and high-level user protection within the Union. There should be no liability where the payer is not in a position to become aware of the loss, theft or misappropriation of the payment instrument. Moreover, once users have notified a payment service provider that their payment instrument may have been compromised, payment service users should not be required to cover any further losses stemming from unauthorised use of that instrument. This Directive should be without

In the absence of gross negligence there could well be an obligation on the part of the home bank to make quasi-total refunds to their client (Complainant). The banks' obligations for effective transaction monitoring are direct and specific under the EU Directive PSD 2. On the other hand, the transaction monitoring obligations on CASP/VFA result only from general fiduciary duties, and are less direct and forceful than those applicable to banks.

If re-imbursement of losses is denied by the home bank on the basis of gross negligence on the part of the Complainant, the same gross negligence would exempt Foris from being a clear direct cause of his claimed losses.

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 as he has failed to provide any evidence of direct causation of the breaches of fiduciary duties to the loss incurred.[39]

In the absence of such evidence, there is the risk that other parties are found potentially primarily responsible for this loss, so that if the Arbiter were to award any compensation without full information on the responsibility of other actors in the fraud journey, this could lead to undue enrichment.

It is in fact strange that the claim against the home bank was filed more than one year after the complaint filed against Foris and was only filed after the first hearing when the Arbiter insisted on provision of evidence of such claim. The Arbiter questions whether this is a case of forum shopping given that logic would have first suggested a priority claim on his home bank given their clear transaction monitoring duties under the PSD 2.

It is quite possible that the home bank could have warned Complainant on the risk of fraud during the payments journey and that their warnings were ignored in a manner that could prove gross negligence on the part of Complainant. This could explain why the case against the home bank was filed

prejudice to payment service providers' responsibility for technical security of their own products. (emphasis added by Arbiter)

[39] This line of reasoning was included in decision AFS 042/2024, which decision was confirmed by Court of Appeal (inferior jurisdiction) case ref 35/2025 file:///C:/Users/mifsa208/Downloads/28_01_2026-35_2025-158407%20(1).pdf

a year after the complaint of Foris and as explained above, was only filed after the first hearing with quite some confusion on the actual date (complaint dated 23 October 2025 attached to an email dated 10 October 2025).

The Arbiter finds lack of good faith on the part of Complainant that whilst filing this complaint and demands substantial compensation from the Service Provider, he failed to attend the hearings and makes himself available to answer under oath cross-examinations questions.

In the circumstances, the Arbiter has serious doubts whether the facts in the complaint form signed by Complainant do in fact tell the whole story of the claims he made on his home bank that, as above explained, have direct primary responsibility for transaction monitoring and for refund of the loss, saving gross negligence on the part of the Complainant.

For the above reasons, this complaint is not upheld and no compensation is being ordered.

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

Alfred Mifsud
Arbiter for Financial Services

<u>Information Note related to the Arbiter's decision</u>

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. Personal details of the Complainant(s) will be anonymised in terms of article 11(1)(f) of the Act.