Before the Arbiter for Financial Services

Case ASF 139/2025

FN

('the Complainant')

vs

Foris DAX MT Limited

(Reg. No. C 88392)

('Foris' or 'Service Provider')

Sitting of 17 April 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 Crédit Mutuel to his account with Service Provider) to a fraudulent platform, has caused him a financial loss for which he is seeking compensation of €220,590.62.[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 fraudulent persons who purported to be representatives of NIXSE investment platform on which he registered on 29 June 2023 with an initial deposit of just €500.

[1] Page (p.) 4

[2] P. 1 - 7 with supporting documentation on P. 8 - 18.

He claims that in total he invested €220,590.62 through 5 transactions as shown in the Table below which were credited to his account with the Service Provider that was opened on 04.08.2023.

Sequence Number	Date	Amount in EURO	Received by Service Provider
1	24.08.2023	50,000	p. 26
2	14.09.2023	78,918	p. 27
3	28.09.2023	75,000	p. 28
4	28.12.2023	15,000	p. 29
5	28.12.2023	1,876	p. 29
As per Complaint	**Total**	**220,794**	

NOTE 1: The amounts in the Table are sourced from the Service Provider's reply. The amounts vary slightly from the claim in the Complaint which show a slightly lesser amount.

NOTE 2: The dates of the payments in the Complaint show approximately the same day and month but in 2024. During the course of the hearings, it was established that these payments were all effected in 2023.[3]

The Complaint also explains that following these payments, the Complainant continued to make other 'investments' in 2024. He mentions a payment for €400,000 transferred on 18 June 2024 when he was promised a reward of €1,000,000 which he could withdraw within a few days. In the report that Complainant filed with the French Public Prosecutor, he mentions a total loss through this fraud scheme of €602,768.[4]

However, it is to be made clear that this Complaint relates to the payments listed in the Table above as subsequent payments were not handled through Complainant's account with Foris.

[3] P. 61 - 62
[4] P. 45 - 47

The timeline of the fraud seems to be:

- August – December 2023 – payments subject to this Complaint circa €220k
- Other payments up to June 2024 – circa €400k bringing total loss to circa €603k.
- July 2024 – on realisation of the fraud case referred by Complainant to French lawyers.
- October 2024 – filed report with French Public Prosecutor
- November 2024 – filed complaint with Société Générale[5]
- March 2025 – Complaint filed with Foris (Crypto.com) following discovery of their involvement in the payments journey.[6]
- July 2025 – Complaint filed with OAFS.

From the Reply of Foris referred to hereunder, it results that each of these fund transfers was immediately converted to crypto assets and then transferred to an external wallet ending ……. *nkqnn,* so that by the end of the process, the Complainant had transferred 8.43333884 BTC (Bitcoin) between 25 August 2023 and 28 December 2023.[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.

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 gross negligence as he had not disclosed any personal data to third parties.[9]

He then quotes various transaction monitoring obligations related to banks and finally concludes as follows:

[5] P. 53 - 58
[6] P. 8 - 15
[7] P. 30
[8] P. 9 - 12
[9] P. 11

"In this case, (Complainant) made no mistake. He did not disclose any personal data to third parties. Consequently, CRYPTO must return the funds to (Complainant) 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.*

- *Foris MT Limited additionally offers the product and services of the Crypto.com Visa Card. The Crypto.com Visa Card is a prepaid card that functions similarly to a debit card. Unlike debit cards, which are directly linked to an individual bank account, the Crypto.com Visa Card is topped up through bank account transfers, other credit or debit cards, or cryptocurrency.*

- *(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 4 August 2023.*

[10] *Ibid*.
[11] P. 25 - 32 with attachments from p. 33 - 41

- *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*."[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 (BTC) and transferred out to the external wallet 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 address the funds were transferred to, does not belong to the Company and as such, any due diligence of the ownership of this address falls under the responsibilities of the provider of said wallet.

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

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 & Conditions.

Please see the relevant section of the Terms & Conditions for your reference:

'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

[12] P. 25

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.

…'

Service Provider's Warnings

In the course of the Complainant's Disputed Transactions, the Service Provider would have provided a number of warnings regarding withdrawals to non-custodial wallets.

The first of these warnings appears whenever a user adds a new withdrawal address to the Cryto.com App. For the reference of the Tribunal, the warning appears a below, in Fig. 15. This warning invariably appears whenever the adding of a new withdrawal address, known as "Whitelisting" occurs, and takes the form of a full screen pop-up.

A similar warning appears at the time of each withdrawal, whether or not the withdrawal address is newly whitelisted or to a withdrawal address which has

already been whitelisted on a previous occasion. An example of this warning can be found below, exhibited as Fig. 16.

As can be seen from the examples provided below, both pop-up warnings specifically warned the Complainant against scams and not to whitelist or withdraw digital assets to investment platforms touting unrealistically high returns, people the Complainant did not know well and to any source the Complainant did not have complete confidence in. In respect of the warning displayed during 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 takes users to the regularly updated Crypto.com Help Center page "Avoiding Digital Currency Scams" (a screenshot of the current page https://help-crypto.com/en/articles/6484926-avoiding-digital-currency-scams is labelled Fig. 17 in the Appendix).

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 they accepted the risks involved and took full responsibility for the 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 the External Wallets.

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

Summary

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 an external wallet address which he nominated.

As outlined above in the Foris DAX MT Limited Terms & Conditions, 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 25 November 2025, the Complainant failed to make presence and was represented by his French counsel. The hearing was postponed to 13 February 2026 but in the meantime, the Complainant's lawyer was invited to submit English translation of any police report and claims on French banks originating the transfers.[14]

At the second hearing of 13 February 2026, the Complainant was present and confirmed the evidence in his Complaint. He was cross-examined as follows:

'***It is said that in my complaint, I mentioned that registered on the NIXSE platform after making an initial deposit of €500, where shortly after, I was contacted by a certain Jules Philippe. And then, there was a number of correspondence with Mr Philippe to assist in the transaction.***

Asked whether it is correct to say that Crypto.com, at this stage, did not enter into any contractual arrangements that I had with NIXSE and was not part of the correspondence that I had prior to the investment that I speak of, I say, no.

Asked how I communicated with Mr Philippe, whether I ever met him in person or only communicated through WhatsApp or emails, I say, I communicated with him by email. I never met the person face to face.

It is said that after the initial deposit of €500, I made an initial success and was proposed a credit contract of €50,000 which kept on increasing to €78,000 and €87,000 and so on.

[13] P. 30 - 32
[14] Submitted 05.12.2025, p. 45 - 58

Asked whether throughout all these transactions I sought advice from anyone else apart from NIXSE, since the amount of money going in these transactions was quite substantial, I say, I did not and I think that if I had, I would not have continued with this scam.

I am refered to what I mentioned that I had to take a loan, and asked whether I took out the loan from a bank or was it a NIXSE arrangement, I say that it was through NIXSE.

Asked whether my personal bank was aware that these transfers were made for crypto investments or to NIXSE, I say, yes.

Asked whether my bank gave me any warnings advising me to be careful when investing in crypto, I say that my bank, Crédit Mutuel, mentioned to me the risks but Société Générale did not.

Asked whether I took any formal proceedings against the bank, I say, yes, against Société Générale. I say the complaint was filed a year ago, but I still have received no response from them.

I am asked wheher I have asked for a follow-up on this complaint with the bank.

Mr Alexandre Dakos replies:

A mediation has been held and we are waiting for a definitive response.

A follow-up has been made and the mediator said that they had received the elements from the bank.

Hence, they are in the final stage to make a decision which will probebly be given shortly.

We asked the Société Générale mediator regarding some elements in June 2025 but he has not responded yet.

Asked whether the payments in question were made from Société Générale, I say, part of it.[15]

[15] P. 59 - 60

At this stage, the Arbiter sought and obtained confirmation that the payments subject of this Complaint were made through Crédit Mutuel against whom no complaint has been registered as they had issued Complainant with suitable warnings at the payments stage.[16]

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

'The Complainant became a client and user of the Service Provider on 4 August 2023, and as discussed, the disputed transactions relate to four withdrawals of Bitcoin cryptocurrency which were purchased in the Crypto.com app account and sent to a single external wallet address between 25 August and 28 December in 2023.

This wallet address is what we call a non-custodial address, and they are not serviced by Crypto.com or identified from data on the blockchain as provided services of other companies of a similar nature.

From the evidence at hand, and the agreement of the Complainant and his legal representatives, these transactions were fully authorised by the Complainant and made pursuant to the Complainant's instructions.

With regard to the warnings, as described in the Service Provider's reply, in the course of the Complainant's disputed transactions, there were a number of warnings provided in place at the material time regarding the withdrawals to external wallet addresses. As this has been detailed in our reply, this will not be repeated here.

In spite of these numerous warnings mentioned at the whitelisting and withdrawal stages, the Complainant proceeded to make the withdrawals to the external wallet whilst negligently disregarding these warnings.

Lastly, there was nothing in our own controls, as well as the controls of our third-party monitoring tools, to indicate that there was any malicious or scam activity involved in these cases at the material time. The Complainant's concerns regarding the disputed transactions were not communicated or

[16] P. 60 -61

brought to the attention of the Service Provider until well after these transactions had already been completed.

Insofar as the transactions have been completed to the full satisfaction of what we were asked to execute on behalf of the Complainant, the Service Provider does not bear any responsibility for any loss in regard to these transactions.'[17]

The Service Provider further denied they had any connection with NIXSE and that they did not provide the wallet address where the crypto was transferred. They assume this was provided by NIXSE.

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

The Arbiter demanded that Foris submit KYC documentation of Complainant at onboarding stage[18] and any exchanges with him during the course of the payments subject of this complaint.

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

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

[17] P. 63 - 64
[18] Received later P. 77 - 78

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'*[19] 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

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

typical services provided to millions of users by operators in the crypto field such as the Service Provider.

- Furthermore, it has not been demonstrated nor emerged that the alleged fraudster to whom the payment was made by the Complainant, was another *Crypto.com* App user and, thus, a client of the Service Provider in the first place. The transfer was rather indicated to have been done to an *'external wallet'* and hence the Service Provider had no information about the third party to whom the Complainant was transferring his crypto.

- The Complainant seems to have only contacted the Service Provider well 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.

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 …'.[22]

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,

[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
[22] P. 65

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'*.

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. 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

[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

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.

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[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]*

[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

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:

> *"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

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

applied to the Service Provider at the time of the disputed transactions in 2022, provides that:

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

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

> *"14. (1) A subject person having the control of assets belonging to a client shall safeguard such assets and the interest of the client therein.*
>
> *…*
>
> *(7) The subject person shall make appropriate arrangements for the protection of clients' assets held under control and shall ensure that such assets are placed under adequate systems to safeguard such assets from damage, misappropriation or other loss and which permit the delivery of such assets only in accordance with the terms and conditions of the agreement entered into with the client."*

The Arbiter is of the view that for the general fiduciary obligations to apply in the context of the VFA ACT, there must be something which is truly out of the ordinary and which should really act in a conspicuous manner as an out-of-norm transaction which triggers the application of such general fiduciary duties.

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

1. The KYC documents submitted by the Service Provider at the request of the Arbiter are mere proof of identity documents and have no real KYC information about the Complainant. There is no information about the Complainant's wealth, annual income and experience in dealing with crypto assets.

2. The failure to obtain substantive KYC documents as above explained may be tolerated in case of clients investing moderate amounts. However, in this case the Complainant's account turnover showed deposits exceeding euro two hundred thousand between 24 August 2024 and 29 September 2024. This merited a much deeper KYC exercise before proceeding further.

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* existing 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]

[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/

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 Complainant 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 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.[34]

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 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[35] without taking any advice or precautions.

[33] EU Directive 2015 - 2366

[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

[35] P. 47 speaks of balance of €3,160,000

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 PSD 2,[36] 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.

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.

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

In this case, the Complainant admitted that Crédit Mutuel, the French Bank that funded the payments subject of this Complaint, had issued warnings to the Complainant and that for such reason, he has not opened any proceedings against Crédit Mutuel.[37]

If reimbursement 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. Having disregarded warnings issued by his home bank, it is unlikely that Complainant would have heeded warnings issued by Service Provider on the very same transfer payments.

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.[38]

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

[37] P. 60 - 61
[38] 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

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