Before the Arbiter for Financial Services

Case ASF 103/2026

TR

('the Complainant')

vs

Foris DAX MT Limited

(Reg. No. C88392)

('Foris' or 'Service Provider')

Sitting of 30 October 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 La Banque Postale to his account with Service Provider) to a fraudulent platform, has caused him a financial loss for which he is seeking compensation of €152,500[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 called themselves Eva Maurice, Mr Lefort and Laurent Bentaled, representatives of the 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 Arbiter has no competence against NIXSE, whoever they may be, this

[1] Page (p.) 5

[2] P. 1 - 9 with supporting documentation on P. 10 - 105.

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 €152,500 through 48 transactions between 24 April 2023 and 22 February 2024 as shown in the Table below which were credited to his account with the Service Provider that was opened on 19 April 2023[3].

Value in Euro	No. of payments	Amount in Euro
500	1	500
1000	1	1000
1500	1	1500
2000	6	12000
2500	1	2500
3000	37	111000
25000	1[4]	25000
Total	**48**	**153500**[5] [6]

These payments were acknowledged in the reply of Foris (see later) who also acknowledged additional payments of €5 on 06.05.2023; €1,000 on 06.08.2023 and €1,000 on 18.09.2023 which do not feature in the La Banque Postale statements and have not been included in the amount of the Complaint.

Foris also acknowledged a deposit of digital assets USDT 538.72 on 23.05.2023[7].

For all intents and purposes, the Arbiter is considering the claim amount of €152,500 as the subject matter of this Complaint by way of compensation sought.

[3] P. 110
[4] P. 63 payment effected on 09.06.2023 acknowledged by Foris on 12.06.2023, p. 119
[5] These payments were confirmed from statements of Complainant's account with La Banque Postale, p. 57 - 79
[6] Complainant indicated total payments amounted to €152,500
[7] P. 116

The amount of €152,500 also features in the claim made by Complainant on La Banque Postale[8]. The French Public Prosecutor[9] refers to an amount of €152,750.

It was reported that an amount of €48,000 was made under pressure when Complainant tried to withdraw his investments and was informed by the scammers that he had to pay these fraudulent fees explained as Blockchain tax, flat tax, and all-risk insurance. It is assumed that these €48,000 are included in the above-listed payments and the compensation claimed for €152,500[10].

Complainant realised that he was being scammed when fraudsters requested a further payment of €8,600 for brokerage fees to refund him €151,480 whilst his account balance was showing €171,939[11].

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.[12]

Complainant denied he was guilty of negligence and explained that he had no intention of transferring his money for purposes other than investment and that the Service Provider (whom he at times refers to as a bank) failed to note the unusual nature of the transfers[13]. He then quotes various transaction monitoring obligations related to banks and finally concludes as follows:

"In this case, Mr. (Complainant) made no mistakes. He did not disclose any personal data to third parties.

As a result, our client's platform, CRYPTO.COM, must refund the funds to the client, as the latter committed no fault."[14]

[8] P. 194 - 196; 198 - 201.
[9] P. 209 - 216
[10] P. 11
[11] *Ibid*.
[12] P. 11 - 14
[13] P. 12
[14] P. 14

Service Provider's reply

Having considered in its entirety, the Service Provider's reply[15]

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.*

- *Mr. **'Complainant'**, e-mail address ……@outlook.fr, became a customer of Foris DAX MT Limited through the Crypto.com App and was approved to use the Wallet on 19 April, 2023.*

- *The Company notes that in the submitted complaints file, the Complainant's representative has outlined the desired remedy as: (i) reimbursement for incurred financial losses.*[16]"

The Service Provider then provided a timeline for the transactions of the Complainant's account with them. These included the above-listed inward transfers of Euro fiat currency. These funds were then converted to crypto assets and transferred out to three external wallets with codes ending ….11284, ….5DCBF, and ….61e58 through at least 22 separate transfers amounting to USDT 164,385.7 between 25 April 2023 and 22 February 2024[17].

[15] P. 110 - 144 with attachments from p. 145 - 187.
[16] P. 110
[17] P. 141

The Service Provider concluded that:

> *"Based on our investigation, the Company has concluded that we are unable to honor the Complainant's refund request based on the fact that the reported transfers were made by the Complainant himself.*
>
> *While we sympathize with the Complainant and recognize that he may have been misled or induced into transferring funds to an alleged fraudster, it is important to note that these transfers were made solely at the Complainant's request. We must also emphasize that the addresses the funds were transferred to, do not belong to the Company and as such, any due diligence of the ownership of these addresses falls under the responsibilities of the provider of said wallet.*
>
> *Unfortunately, Crypto.com cannot revoke any virtual asset withdrawals because blockchain transactions are fast and immutable.*
>
> *The Complainant is solely responsible for the security and authenticity of all instructions submitted through her Wallet as outlined in the Foris DAX MT Limited Terms of Use.*
>
> *Please see the relevant section of the Terms of Use for your reference:*
>
> *'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 it 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 numerous warnings regarding withdrawals to non-custodial wallets which were introduced in June 2023.

The first of these warnings appears whenever a user adds a new withdrawal address to the Crypto.com App. For the reference of the Tribunal, the warning appears as below, in Fig. 98. 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. 99.

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. 100 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 Wallets. 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 wallets and the fact that they are 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.[18]"

[18] P. 142 - 144

Hearings

At the first hearing on 13 July 2026, the Complainant largely restated his case as explained in his Complaint and confirmed he never received any funds following his payments to settle fees and taxes. He was only provided with a prepaid card which allowed him to pay for a restaurant meal and withdraw €100.

Under cross-examination he said:

> ***"I am referred to what I said in my complaint that I saw an advert for the site NIXSE.COM and requested information.***
>
> ***Asked whether it is correct to say that I requested information from NIXSE.COM directly about NIXSE.COM, I say, yes. I was in contact with NIXSE.COM directly.***
>
> ***It is said that in my complaint I mention Mr Pekin, Ms Maurice among other individuals on page 81 of my complaint.***
>
> ***Asked whether all these individuals identified themselves as employees or personnel representing NIXSE.COM, and whether I ever met any of these advisors in person, I say, yes, they identified themselves as working with NIXSE as brokers and advisors. And Ms Maurice said that she was a supervisor with NIXSE. But I never had met any of these representatives in person.***
>
> ***It is said that before signing any of the contracts mentioned on page 4 of the complaint, there is the credit agreement, the beginner agreement, the data requirements agreement, etc.***
>
> ***Asked whether I sought any professional, financial advice or whether I had any experience in crypto trading before, I say, no, I did not ask for professional, financial advice.***
>
> ***At first, it started with a unit contract, and after that they told me that I should sign up for a loan, and so on.***
>
> ***It is said that on page 19 of my complaint, there is an email dated 12 March 2024, which I sent to NIXSE.COM in which I said:***

'You offered me the option to close my account and I decided to do so in December 2023.'

I am asked whether I continued to make further and additional transactions after this date where there were transactions made in January on the 9th, on the 10th, on the 12th, on the 22nd, on the 2nd of February 2024, 5th February, 19th and 22nd.

Asked, if I decided to close my account in December 2023, why did I not mitigate my damage and try and withdraw that fund, but rather continued to invest and make transactions into an account which I said I closed, I say that I did not make any transactions after I closed my account. After that, the scammers told me that they will buy out my account and, so, my account reappeared. And that is why I continued to invest in the hope that …

It is said that on page 4 of my complaint, I refer to the AnyDesk application.

Asked whether it is correct to say that I installed this application on my device, and whether I knew at the time that I was giving them access to my device, to my laptop, when I installed this application, I say, no. They told me to install AnyDesk in order to communicate with them. Yes, I did install it.

Asked whether I filed a police report about this fraud that I had suffered, I say, yes.[19]"

…..

"Asked whether I file a complaint with my bank, Banque Postale, from where the transactions emanated, Mr Dakos intervened to state:

We sent a formal notice to Banque Postale in 2024, and after that, we were referred to the ombudsman, but the case is currently pending. There is no decision from the ombudsman yet. It is still ongoing.

[19] P. 189 - 190

I am referred to page 184 of the case file where, in the reply of the Service Provider, it states that warnings were given by Foris DAX prior to any withdrawal or transfer.

Asked to confirm whether I had seen or remember receiving these warnings, I say, no, I did not receive these warnings.

I am asked whether prior to pressing 'Confirm' or any similar button before executing the transaction, I recall seeing these warnings, I say, no.

Asked by the Arbiter to confirm whether I authorised all the transactions from my French bank to Crypto.com, I say that I authorised the payments from Banque Postale to Crypto.com but after that the scammers transferred by means of AnyDesk the funds from Crypto.com to NIXSE platform.

The Arbiter states that this could be the reason why the Complainant was not seeing these warnings because these warnings were generated when the scammers were making these payments on behalf of the Complainant using AnyDesk application.

I say, yes, I was not seeing these warnings.

I say, yes, I was seeing these payments appearing on the investment platform.

It is said that there were many payments, but they were all under €3,000 - €1,000, €500; one time there was a payment for €9,000 - but then, on 12 June, there was the only payment over €10,000 which was for €25,000.

Asked whether I remember this large payment, I say that this payment of €25,000 was for flat tax. The scammer told me that I would be able to withdraw my money after paying that tax.

The scammer told me that this money will allow me to being part of a group of multiple investors.

The Arbiter states that now, if he understood correctly, the payment of €25,000 was for joining a special class of investors with some privileges.

Asked whether this is correct, I say this is correct.[20]***"***

Following the hearing, the Complainant's legal advisers submitted a copy of:

- the claim made against La Banque Postale dated 23.02.2026[21].
- the claim made with the Consumer Ombudsman dated 11 June 2026[22].
- the report dated 30.05.2024 to the Public Prosecutor about the fraud[23].

A second hearing was held on 27 July 2026 for the evidence of the Service Provider through Pema Fung who stated:

"The Complainant became a client and user of the service provider on the 19th of April, 2023. The disputed transactions in question relate to 22 transfers of cryptocurrency, which were purchased in the Complainant's Crypto.com app account and sent to three external wallets over a period of nearly 10 months between the 25th of April, 2023 to the 22nd of February, 2024.

These wallet addresses are what we call non-custodial addresses, meaning they are not serviced by Crypto.com or, as identified from data on the blockchain, as serviced or provided by other cryptocurrency exchanges of the same nature.

From the evidence at hand, and the agreement of the Complainant in his oral evidence, the Complainant had granted control of his mobile device and, therefore, his Crypto.com app account, to the alleged fraudsters through the remote software, AnyDesk, to perform transactions on his behalf.

Further, the Complainant acknowledges he was aware of these transfers and Service Provider that he was seeing these payments appearing on the investment platform.

[20] P. 191 - 192
[21] P. 198 - 202
[22] P. 194 - 197
[23] P. 209 - 216

For the avoidance of any doubt, the Service Provider has no affiliation whatsoever with the NIXSE platform or the individuals mentioned, namely, Mr. Pekin, Ms. Eva Maurice, or Mr Lefort.

With regard to the warnings the Service Provider issues within the Crypto.com app, this has been detailed in the Service Provider's reply and will not be repeated here.

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 transactions at the material time. The Complainant's concerns regarding these withdrawals were not communicated or brought to the attention of the Service Provider until these transactions had already been completed.

The Service Provider would like to mention the larger payment of €25,000 being a withdrawal of 26,090 USDT that was mentioned during the first sitting on the 13th of July 2026.

The Service Provider would like to add that leading up to this particular withdrawal, which occurred on the 12th of June 2023, six previous withdrawals totaling 42,560 USDT were made without any issues or complaints. These were all made to the same external wallet address. Insofar that the transactions have been completed to the full satisfaction of what the Service Provider was asked to execute on behalf of the Complainant. The Service Provider submits that it does not bear any responsibility for any loss in regard to these transactions.

Lastly, for the record, as Doctor Bencini has correctly pointed out, the Complainant's legal advisers at the first sitting have stated that a formal notice was sent to Banque Postale in 2024. However, from the documents provided by the Complainant's legal representatives, which were received by us today, the earliest record of any formal notice, or any correspondence at all, to Banque Postale was not made until February 2026.

> ***From all the evidence submitted until now with regard to this complaint, it appears that in 2024 the only notice issued by the Complainant was to Foris DAX MT Limited, the Service Provider.***[24]***"***

On being cross-examined, Pema Fung continued:

> ***"Asked whether Crypto.com was aware of the fraudulent nature of the external wallet, I say, no. As mentioned in my evidence just now, at the material time, Crypto.com or the Service Provider itself was not aware of any fraudulent nature of the wallets.***
>
> ***Asked why Crypto.com did not send an alert and advise Mr Complainant of the abnormality when he created a new account that was quickly funded, I say that, as mentioned in our evidence, we did not find any abnormalities in the way Mr Complainant's account was being operated.***
>
> ***His transactions had gradually built to the amounts they had become and there were no reports from Mr Complainant of any fraud, fraudulent activity or the fact that he had been subjected to fraud until much later after his account had been opened and used for 10 months. Further, none of our third-party service providers have flagged any of the wallet addresses that Mr Complainant had sent his funds to either.***
>
> ***Lastly, many people use the exchanges so that they can onboard fiat funds, purchase crypto and transfer them to different crypto wallets. That is a huge purpose of what crypto exchanges function as. And Mr. Complainant's use of the account fell within the normal usage of such.***
>
> ***Asked why Crypto.com did not verify the consistency of Mr. Complainant's profile, his age, his inexperience in crypto money activity and the suspected operations, I say that from our internal investigations, we did not see any abnormality in respect of Mr Complainant's profile and his transactions.***[25]***"***

[24] P. 203 - 205
[25] P. 205

The Arbiter demanded that Foris submit the documentation re KYC of Complainant at onboarding stage[26].

These were identification documents and statements as follows:

Expected annual turnover	€ 20,001 – 60,000
Annual Income	€ 80,001 – 100,000
Occupation	Manager_ business owner.

Final Submissions

In their final submissions,[27] 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 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.

[26] P. 218 - 220
[27] P. 222 - 223 Complainant; p. 225 - 227 Service Provider.

The Arbiter further notes that in the year 2020, the MFSA has also issued a *'harmonised baseline guidance on Technology Arrangements'*[28] 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 either directly or through giving AnyDesk access to the scammers (which from the point of view of Foris appeared as normally authorised by Complainant).

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 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

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

the first place. The transfer was rather indicated to have been done to *'external wallet(s)'* and hence the Service Provider had no information about the third parties 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.[29]

  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).[30]

  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 …'.[31]

  Based on 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:

[29] 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).
[30] E.G. https://www.chargebackgurus.com/blog/chargebacks-more-volatile-complex-than-cryptocurrency
[31] P. 17; 142 - 143

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'*.[32] 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[33] and Travel Rule[34] 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 - 2024.

[32] 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'*

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

[34] 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

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[35] 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),[36] 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.[37]*

[35] *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

[36] Such as Case ASF 158/2021

[37] Such as Case ASF 069/2024

Compliance with such recommendations or lack thereof will be taken into consideration in future complaint adjudications."[38]

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."[39]

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****;…"*[40]

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 2023/4, provides that:

[38] Emphasis added by the Arbiter
[39] Emphasis added by the Arbiter
[40] Emphasis added by the Arbiter

"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 was no event which was out of the ordinary to a degree which should have triggered the application of the fiduciary duties of the Service Provider.

As explained in the Table of Payments above, most payment flows were in relatively small amounts not exceeding €3,000. There was only one payment for a rather large amount of €25,000. This was executed after 14 smaller payments had been executed in the previous 7 weeks for a total of €40,000.

This payment brought the cumulative total of payments to €65,000 which was close to the upper indication of €60,000 annual turnover and, understandably,

did not raise any reason to suspect fraud considering that Complainant had declared an annual income of €100,000 and that he was a business owner.

Following this large payment, the flow of small payments continued for a further 8 months in small shots never exceeding €3,000.

One might argue whether the total payments of some €150k over 10 months compared to the declared annual turnover of €60k should have raised any suspicion of fraud. Given that these payments were clearly sourced from his own account with a reliable French bank and that they were spread over two calendar years, and given the small value of the majority of the transactions, the Arbiter sees no failure of fiduciary duties on the part of Foris.

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.[41]

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.

[41] 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/

In fact, the Arbiter notes that in his Complaint, the Complainant refers to provisions of the PSD 2,[42] 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.[43]

The Arbiter considers that the dominant causes for this loss are:

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

2. Possibly, the home bank failed to spot the fraud and issue a 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.

[42] EU Directive 2015 - 2366

[43] https://www.eiopa.europa.eu/document-library/other-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

In terms of preamble 71 of the said PSD2, 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.

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.

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.

It is in fact strange that the claim against the home bank was filed twenty-one months after the complaint filed against Foris[44].

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.

[44] P. 10 complaint against Foris dated 30.05.2024; p. 198 complaint against La Banque Postale dated 23.02.2026

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

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.