Before the Arbiter for Financial Services

Case ASF 281/2025

US

('the Complainant')

vs

Foris DAX MT Limited

(Reg. No. C 88392)

('Foris' or 'Service Provider')

Sitting of 30 June 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 Banco BPM in Italy to his account with Service Provider) to a fraudulent platform, has caused him a financial loss for which he is seeking compensation of €284,795 being the amount of funds actually transferred amounting to €115,520 and profit he would have made on his supposed purchase of BTC 2.531 units based on a price of US$112523.49 at the time of making the Complaint.[1] [2]

The Complaint[3]

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 herself Eleni Argos of Greek origin.

[1] Page (p.) 4
[2] Price of BTC presently is below USD70,000 so this profit, even if it were real, has substantially diminished.
[3] P. 1 - 8 with supporting documentation on P. 9 - 203.

She claimed to specialise in trading in investments with both Trade Baionics and Vestletrade on the XTB platform. This lasted from 13 January 2022 till September 2022.

On 11 April 2022, Alessandro Rossi became his account manager, and he was guided to make transactions worth €115,250 via a Lithuanian intermediary Transactive System UAB.

During the proceedings:

1. The Arbiter made clear he will not consider a claim related to alleged loss of profits that would have been made if the transactions were not fraudulent so that he will only consider the complaint related to €115,250 actually 'invested' by Complainant.[4]

2. Transactive System UAB only handled payments for the period from 24 March 2022 to 18 January 2023 in respect of 13 transfers amounting to €53,750.

3. Transactions for the period after 18 January 2023 until 16 March 2023 involving 6 transfers for €64,400 were made through a Malta registered intermediary.

4. Transactions as in 2. and 3. amount to €118,150 compared to a claim of €115,520 as these funds were routed to the account that Complainant had with Crypto.com (brand name of Foris) and from there somehow spirted away to external wallets controlled by fraudsters.

5. This complaint is part of a much larger scam amounting to €341,550[5] including a loss incurred in 2018 for €161,900.

Following request for more information by the Arbiter,[6] Complainant informed:[7]

a. His education level was that of an accountant and his profession was that of artisan entrepreneur.

[4] P. 414
[5] P. 286 - 288
[6] P. 250- 251
[7] P. 254 - 256

b. He had no experience in financial markets.

c. He has never opened an account with Crypto.com.

d. At the time of the last transfer of April 2023 his investment platform was showing a profit of about €400,000.

e. No claim was made against the home bank Banco BPM.

Service Provider's reply

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

Where the Service Provider provided a summary of the events which preceded the Complainant's formal complaint and explained and submitted the following:

"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.*

- *(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 14 March 2022.*

- *The Company notes that in the submitted complaints file, the Complainant's representative has outlined his desired remedy as: (i) reimbursement for incurred financial losses*."[9]

[8] P. 207 - 228 with attachments from p. 229 - 249.
[9] P. 207

The Service Provider then provided a timeline for the transactions of the Complainant's account with them. These included above referred to inward transfers of Euro fiat currency through a Lithuanian and a Maltese financial intermediary. These funds were then converted to crypto assets and transferred out to six different external wallets with addresses ending:
…CpScJB
…xr6j7x
…jaJCo8
…BJ6kHy
…FoGGMk
…pmuvh2

In total, they report transfer involving BTC[10] 5.56063585.

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:

[10] BTC is abbreviation for Bitcoin, the most popular digital asset.

"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.

…"

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 external wallet addresses which he nominated.

As outlined above in the Foris DAX MT Limited Terms of Use and as accepted pursuant to each withdrawal warning, 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. This is particularly emphasized against the backdrop of each warning that the Complainant has received upon every whitelisting and withdrawal transaction.[11]

Hearings

At the first hearing on 18 March 2026, the Complainant stated:

"***I say that they opened an account with Crypto in my name. I say I have an account with Crypto but I did not open it myself. It was Mrs Eleni who opened an account in my name with Crypto.com. And you can find the e-mail on the 10th of March that she sent all details of Openbank or open an account in crypto.***

The account in my name was opened by the fraudster. I sent money to this account which was opened by the fraudster, but I have no idea where my money finished off.

I believe that the money was sent to Crypto in my name but I do not know where the money has gone.

The Arbiter points out that the information that the Complainant is seeking is in the reply of the Service Provider."[12]

Under cross-examination, he confirmed that:

1. None of the fraudsters identified themselves as representing Crypto.com.

[11] P. 227 - 228
[12] P. 414 - 415

2. He gave to Eleni scanned documents of his ID card, bank statement and utility bill for her to use to open accounts in his name.
3. He has no access to his Crypto.com account.
4. His email address registered on his Crypto.com account was correct.
5. He did not send selfie or live video within the Crypto.com app during the account opening process and that all such procedures were performed by Eleni.
6. All his attempts to withdraw funds from the fake platform were unsuccessful.
7. He did not seek professional advice about these investments as he was seeing good profits and did not realise that it was a scam.
8. He remembers receiving email notifications from Crypto.com regarding transactions on his account.
9. He was not seeing the funds transferred from Banco BPM arriving on his Crypto.com account. He had given AnyDesk access to Eleni who had full access to his Crypto.com account and she was making the fraudulent transfers from his Crypto.com account through AnyDesk which would then show up on his Trade Baionics platform.

A second hearing was held on 22 April 2026, where Pema Fung testified on behalf of the Service Provider stating:

"The Complainant became a client of the Service Provider on the 14th of March 2022. During this account opening process, [the Complainant] submitted a copy of the front and the back of his ID card as well as providing a selfie that was taken through the Crypto.com app.

This account is registered under the email address xxxxxxx@gmail.com which is the same email account the Complainant provided in his complaint filed with the OAFS.

With regard to the fiat deposits made by the Complainant from his bank account to his Crypto.com fiat wallet, the euro deposits from the date of account opening up until January 18th of 2023 were made to a virtual IBAN

held with Transactive Systems, a Lithuanian-based EMI. This was our fiat wallet provider at the time.

All Euro deposits made after that date were made through the virtual IBAN held with OpenPayd, which is our current Service Provider. We changed our service providers in late January 2023.

The disputed transactions in question relate to the withdrawals of cryptocurrency, which was purchased through [Complainant's] Crypto.com app account and sent to six external wallet addresses between the 25th of March 2022 and the 5th of April 2023.

These wallet addresses are what we call non-custodial addresses, which means that they are not serviced by Crypto.com or identified from the data on the blockchain as provided by similar hosted crypto exchanges.

From the evidence at hand, these transactions were either fully authorised by the Complainant himself or made with the gross negligence of the Complainant, having granted third-party access to his account through remote access software, AnyDesk.

In any event, following each and every euro deposit made from the Complainant's bank account to his fiat wallet, each crypto purchase made with these funds, and each withdrawal of cryptocurrency made from the Complainant's Crypto.com app account, in addition to each whitelisting, an email, as well as an app push notification on most occasions, was sent to the Complainant's registered email address.

We have records of this, and if Mr. Arbiter wishes for us to present these, these can be presented at a later stage. As such, the Complainant would have had notice of all such deposits, purchases, and withdrawals made to and from his Crypto.com app account.

There was nothing in our own controls, nor in the controls of our third-party monitoring tools to indicate that there was any malicious or scam activity involved in any of these transactions at the material time. Further, the Complainant's concerns regarding the disputed transactions were not communicated or brought to the attention of the Service Provider until after these transactions had all been completed.

Insofar that the transactions have been completed to the full satisfaction of what we were asked to execute on behalf of the Complainant through his account, the Service Provider does not bear any responsibility for any loss in regard to any of these transactions, whether made through his own actions or as a result of his gross negligence by granting access of his mobile device to the scammers via AnyDesk."[13]

On cross-examination, she committed to send copies of his selfies and ID that the Complainant used on registration of his account with Crypto.com.[14]

Complainant's representative disputed Pema Fung's claim that an email was sent to the registered address for each transaction of the account. Evidence of such notification was subsequently sent by the Service Provider at the request of the Arbiter.[15]

The Arbiter pointed out that the crux of the Complaint is whether the transfers of the BTC to the wallets controlled by the scammers were correctly authenticated and authorised by Complainant in a way that the Service Provider could not suspect that he was being manipulated by fraudsters.

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

[13] P. 419 - 420
[14] P. 437 - 438
[15] P. 429 - 435

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'*[16] 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 notes that Complainant denies having authorised the fraudulent transfers subject of this complaint. He admits giving the fraudsters full access to conduct transactions on his account Crypto.com as if he was doing them himself.

He even raises doubt if he has actually set up the account with Crypto.com and he said this was all done by the fraudsters to whom he provided identity documents, copies of bank statement and utility bill. He even dared suggest that the copies of the ID and his selfies presented by the Service Provider to prove his onboarding were manipulated by AI.

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

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

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 *'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.[17] [18]

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).[19]

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 …'.[20]

Based on the facts presented during the case, the Arbiter could not conclude that the Service Provider failed to adhere to any specific

[17] P. 9 first contact on 23.05.2024 last transaction date 05.04.2023
[18] 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).
[19] E.G. https://www.chargebackgurus.com/blog/chargebacks-more-volatile-complex-than-cryptocurrency
[20] P. 65

obligation, or any specific regulatory requirements applicable to it, nor did he find any infringement of the Terms and Conditions applicable in respect to the service offered.

In arriving at his decision, the Arbiter considered the following aspects:

i. AML/ CFT Framework

Further to the Prevention of Money Laundering Act (Cap. 373) and Prevention of Money Laundering and Funding of Terrorism Regulations ('PMLFTR'), the Financial Intelligence Analysis Unit (FIAU) issued Implementing Procedures including on the *'Application of Anti-Money Laundering and Countering the Funding of Terrorism Obligations to the Virtual Financial Assets Sector'*.[21]

These are *'sector-specific Implementing Procedures [which] complement the Implementing Procedures – Part I [issued by FIAU] and are to be read in conjunction therewith'*.[22] 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[23] and Travel Rule[24] obligations which entered into force in 2025 and which give more

[21] P. 101 - 102
[22] 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'*
[23] EU Directive 2023/1114 on markets in crypto assets https://eur-lex.europa.eu/legal-content/EN/AUTO/?uri=celex:32023R1114
[24] 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[25] 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),[26] 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*

[25] *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

[26] Such as Case ASF 158/2021

empty the bank accounts of retail customers and disappear such funds in the complex web of blockchain anonymous transactions.[27]

***Compliance with such recommendations or lack thereof will be taken into consideration in future complaint adjudications**."*[28]

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**."*[29]

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****;…"*[30]

[27] Such as Case ASF 069/2024
[28] Emphasis added by the Arbiter
[29] Emphasis added by the Arbiter
[30] Emphasis added by the Arbiter

It is further to be pointed out that one of the High Level Principles outlined in Section 2, Title 1 *'General Scope and High Level Principles'* Chapter 3, Virtual Financial Assets Rules for VFA Service Providers of the VFA Rulebook, that applied to the Service Provider at the time of the disputed transactions in 2022, provides that:

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

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

> *"14. (1) A subject person having the control of assets belonging to a client shall safeguard such assets and the interest of the client therein.*
>
> *…*
>
> *(7) The subject person shall make appropriate arrangements for the protection of clients' assets held under control and shall ensure that such assets are placed under adequate systems to safeguard such assets from damage, misappropriation or other loss and which 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 no event which is out of the ordinary to a degree which should have triggered the application of the fiduciary duties of the Service Provider.

The payments were spread over a period of more than one year (from March 2022 to April 2023) involving some 20 inbound transactions with the highest

individual value of €15,000 and the lowest €1,500 and another 20 outward transactions of corresponding value in BTC.

The pattern of inflows and outflows is not indicative of extraordinary events for a normal customer trading in crypto-assets, certainly not to an extent where fraud should have been suspected. All the funds were being received from the Complainant's own account with Banco BPM without any change of beneficiary.

The only question the Arbiter may raise is that the onboarding process appears to have been a mere exercise of identity without deeper KYC questioning on the income and financial status of the applicant and the expected turnover he was considering when he applied to open the account. However, this is a regulatory issue the Arbiter does not consider as having been a direct contributor to the losses incurred.

The main and direct contributor to the loss is customer gross negligence in trusting fraudsters with full access to his account with Crypto.com, enabling them to transfer customers funds to wallets controlled by them and showing fake profits on the platform. Gross negligence for not seeking any professional advice before parting with his money and in not suspecting fraud when his requests for encashment were not being met.

The degree of gross negligence on the part of the Complainant is unbelievably high considering that in the police report[31] he admits having already suffered a loss of €161,900 through a scam in 2018 and also another recovery scam[32] of €64,400 incurred after the loss subject of this scam at the hands of an unknown lawyer who promised him easy recovery of his losses.

The Arbiter notes that Complainant admits he has made no claim on his home bank related to any failure on their part to warn him about fraud suspicions resulting from their transaction monitoring obligations in terms of provisions of the PSD 2,[33] which whilst applying to banks were at the time not applicable to VFA licensees.

[31] P. 285 - 287
[32] P. 288
[33] EU Directive 2015 - 2366

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, 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' obligation for effective transaction monitoring is 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.

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.[34]

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.

[34] 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/

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.

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.[35]

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 attributable to the Service Provider. In the absence of such evidence, there is 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 no claim was made against the home bank.

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. Banks have a much longer relationship with client than a VFA and are in a better position to spot irregularities and smell fraud from sudden

[35] 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

changes in the payment pattern of a client. In this case, the VFA relationship with Complainant was short with consistent payment pattern.

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.