Before the Arbiter for Financial Services

Case ASF 175/2024

ZE

('the Complainant')

vs

Foris DAX MT Limited

(Reg. No. C 88392)

('Foris' or 'the Service Provider')

Sitting of 30 May 2025

The Arbiter,

Having seen the Complaint made against Foris DAX MT Limited relating to its alleged failure to warn client that his transfer of USDT 21,592.06 and ETH 33.95797[1] to a fraudulent platform has caused him a financial loss for which he is seeking compensation of €77,255[2] being the fiat currency transfers effected to finance the acquisition of the crypto assets transferred to fraudsters.

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 through *Crypto.com* whose misconduct allowed the fraudster operating through trading platform NIXSE to steal his money.

[1] Page (p.) 85
[2] p. 5
[3] P. 1 - 7 with supporting documentation on P. 8 - 73.

He claims to have made 7 transfers totalling €75,000 from his bank accounts in France to his account with *Crypto.com* to invest as pressurised by NIXSE who had promised substantial profits from his investments. These transfers were made as follows:

Date	**Amount in EURO**	**Remitter bank**[4]
08.05.2023	5,000	Boursorama
19.05.2023	30,000	Boursorama
22.05.2023	19,000	Boursorama
22.05.2023	1,000	Boursorama
13.06.2023	2,000	Boursorama
13.06.2023	8,000	Boursorama
13.07.2023	15,000	Boursorama
TOTAL	**75,000**	

From the submitted statement of Boursorama, there appears to be a further payment of €10,000 effected on 03 July 2023 which is not listed as having been received in the submissions made by Service Providers.

The Complainant also made reference to a payment of €2,000 which he states he managed to withdraw on 19 July 2023 but, again, this is not listed as having passed through Foris DAX. These and other transactions may explain the difference between the above-listed payments of €75,000 which were transferred to Service Provider to make his 'investments' under the guidance of the fraudsters and the compensation claim for €77,255

[4] P. 28 - 31

In his Complaint, it was also submitted that Complainant is 52-year-old single father suffering from chronic fatigue and has been off work since May 2022. He claims that fraudsters misled him to make what seemed profitable investments on NIXSE platform, and he was promised easy and high profits which never materialised. Even after making the above-listed payments, the fraudsters still pressured him to make a further payment of €35,000 with a promise that as soon as this was received, there will be a counter transfer in his favour of €356,315.89 for which false proof was provided.[5]

The fraudsters continued to make pressure on Complainant to make further payments but, ultimately, running out of resources, the Complainant realised it was a scam and made a report to the relevant French Authorities.[6]

In his Complaint, he presented extensive documentation of contracts and correspondence exchanged with NIXSE explaining the investment. However, as the Arbiter has no competence against NIXSE, this documentation is quite irrelevant to this Complaint as Foris was not a party to such contracts and had no access to such knowledge at the time when the transfers complained of were being executed.

He maintained that Service Provider should have detected the irregularity of the transactions on his account and, therefore, held them responsible for his 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.[7]

Complainant denied he was guilty of negligence and explained:

'***b. Customer's absence of negligence***

In law, any cryptocurrency exchange platform is required to distinguish between two types of customers. First, a person who is not aware of the risks, generally an individual, will be eligible for the bank's duty to warn. Then, a well-informed

[5] P. 5; 13
[6] P. 65 - 73
[7] P. 14 - 16

person, generally a professional, will be presumed to be aware of the risks associated with investment transactions.

In principle, the payer bears all losses caused by unauthorised payment transactions if these losses result from fraudulent conduct on his part or if he intentionally or through gross negligence failed to meet the obligations mentioned in Articles L. 133-16 and L. 133-17 of the Monetary and Financial Code.

These obligations are:

- *to take all reasonable measures to preserve the security of personalised security data, and*
- *to inform the payment service provider without delay of cases of misappropriation of funds and to stop fraudulent payments.*

However, the burden of proof of fraudulent conduct, intentional breach of duty or gross negligence by the User lies with the Payment Service Provider. Moreover, this proof cannot be deduced from the mere fact that the payment instrument or the personal data linked to it were actually used.

Consequently, the court ruled that in order to prove negligence on the part of the customer and to block his chances of being reimbursed for his loss, the customer must have disclosed to a third party, "intentionally, through recklessness or gross negligence, strictly confidential identification elements that enabled the disputed payments", as the bank could not simply refer to the hypothesis of "phishing", by claiming that the customer had certainly responded to a fraudulent e-mail that he thought was from the bank so that he would fill in a certain number of points including the identifiers, passwords and key codes that allow remote transactions to be carried out, without providing evidence of such negligence (Cour de cassation – Commercial Chamber, January 18, 2017, no. 15-18. 102).

In this case, *(the complainant) wanted to invest his money in a secure manner. He simply followed the announced procedure for making his investment and then the announced procedure for releasing his funds, without committing any fault. In particular, he purchased a volume of 70 lots as indicated by the financial department processing his withdrawal request.*

On the other hand, it was the manoeuvres of the so-called experts on the NIXSE platform that helped to hide the truth from (the complainant), by concealing from him their real intentions, in particular to defraud him and breach his trust.

The technical nature of the fraud perpetrated by the perpetrators, in particular the various insistent telephone calls made in the context of a procedure to release funds, clearly contributed to the theft of (the complainant's) funds, and (the complainant) could not have realised the deception under these conditions.

***Consequently,** you must return the funds to the client, as he was not at fault."*[8]

Complainant also submitted that shortly after making the payment of €50,000 between 19 and 22 May 2023, he was contacted by his bank, Boursorama, ***'as part of their policy against money laundering'***,[9] but it appears that his Bank was not alert to any fraud considerations and, in fact, continued to process his payments as above indicated.

Service Provider's reply

Having considered in its entirety the Service Provider's reply,[10]

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 "Fiat Wallet"), which allows customers to top up and withdraw*

[8] P. 16 - 17
[9] P. 11
[10] P. 79 - 86 with attachments from p. 87 - 94.

fiat currencies from and to their personal bank account(s). This service is offered by the legal entity Foris MT Limited.

- *Mr … (the "Complainant"), e-mail address …….. became a customer of Foris DAX MT Limited through the Cryto.com App and was approved to use the Wallet on 9 May 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.'*[11]

The Service Provider then provided a timeline for the transactions of the Complainant's account with them. These included the above-listed 7 inward transfers of Euro fiat currency collectively amounting to €75,000. These funds were then converted to crypto assets (USDT and ETH) and transferred to two external wallets on the instructions of the Complainant between 10 May 2023 and 15 July 2023.

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.

[11] P. 79

The Complainant is solely responsible for the security and authenticity of all instructions submitted through his Wallet as outlined in the Foris DAX MT Limited Terms of Use.

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

QUOTE

7.2 Digital Asset Transfers

…

(b) Crypto.com processes all Digital Asset Transfers according to the instructions received from you and does not guarantee the identity of any recipient. You should verify all transaction information prior to submitting instructions for a Digital Asset Transfer to Crypto.com as the Digital Asset Transfer may not be cancelled or reversed once processed by Crypto.com unless Crypto.com decides at its sole discretion that the transaction should be cancelled or reversed and is technically capable of such cancellation or reversal. You acknowledge that you are responsible for ensuring the accuracy of any instructions submitted to Crypto.com and that any errors may result in the irreversible loss of your Digital Asset.

…

UNQUOTE

In summary, it seems conceivable that the Complainant has been the victim of an alleged scam. However, due to the nature of the external wallet and the fact that it is not hosted or operated by Foris DAX MT, we can neither confirm nor deny this.

Whilst we fully empathize with (the Complainant) in this regard, it cannot be overlooked that he had willingly, transferred his virtual asset holdings from his Crypto.com Wallet to an external wallet address which he nominated.

As outlined above in the Foris DAX MT Limited Terms of Use, the Complainant is solely responsible for the security and authenticity of all instructions submitted through the Crypto.com App, and as such, the Company cannot

accept liability for the veracity of any third party or for the instructions received from the Complainant themselves.'[12]

Hearings

During the hearings, the Complainant failed to make presence and was represented by his French counsel.

This raised objections from the Service Providers who, in the absence of possibility to cross-examine the evidence submitted by Complainant, claimed that such evidence should not be considered.

The Arbiter ruled that in the absence of Complainant making himself available for cross-examination, he is taking a clear position that the payments and transfers complained of were executed with the full authority of the Complainant, and the Service Provider will only be asked to defend themselves from the claim that through their monitoring systems they should have stopped the transfers to external wallets controlled by the fraudsters as there were clear signs of fraud.

Complainant's lawyers assented to such decision whilst Service Provider wished to register the following statement:

'***I would like to have a general statement in the note verbal of all these cases with regard to the fact that as agreed, the evidence of the complainant was not given; it was given by his representative, and the cross-examination was very limited.***

However, I do not want that to be an acceptance of all the other allegations being made by the complainant. So, I want to make it clear from the service provider's side that the absence of the complainant's testimony is not being taken as an acceptance of his allegations, but it is rather being dismissed and obviously it cannot be considered evidence because he is not available.

So, everything else is being dismissed because the only assumption and the only thing that Foris DAX has accepted is that there is the authorisation of the complainant and that has been accepted; but everything else is not being

[12] P. 85 - 86

accepted, that is, whatever the complainant said for which he has not been called in to testify.'[13]

The Complainant's representative asserted:

'***And we believe that is why we are now in front of the Arbiter because Crypto.com failed to meet several of its obligations by not warning or intervening in this scam. Crypto.com should have warned (the Complainant), as a cryptocurrency exchange platform; it is a financial institution subject to regulatory obligation and it should have recognised that (the Complainant) was being scammed specifically by the Nixse.com platform and not taking the necessary measures to prevent this fraud from happening.***

We have provided supporting documents including the transactions which have been taking place and, so, we believe that beyond the responsibility of (the Complainant's) banks, it was also up to Crypto.com to take certain precautionary measures to protect him but this was not done.

So, today, in our analysis, this company is clearly liable; and this is what we can say about this matter.'[14]

It was established during the first hearing of 17 February 2025, that Complainant intends to open a complaint against his French Bank to hold them responsible for not withholding the transfers he was making to his Crypto.com account.[15]

During the second hearing of 01 April 2025, the Service Provider submitted:

'We can see from the case files that the complainant became a user of the service provider from the 9th of May 2023 and made a series of transactions between the 10th of May 2023 and the 15th of July 2023. He made a number of purchases and then a number of withdrawals, primarily, exclusively, to the two wallet addresses. One wallet address was for the transfer of USDT and also the transfer of ETH.

What we can say about these various transactions at the time they were made is that we have taken out and carried out transaction monitoring as we do for all our transactions. I can confirm that at the date of these withdrawals,

[13] P. 79 in parallel case ASF 190/2024
[14] P. 99
[15] P. 100

nothing can be shown to identify these transactions as transactions that would merit any pause or stop from our side. We can see nothing or no warnings from the side of our different service providers, and we had no other information to question the nature of these transactions.

I will also point out that in the case of these transactions, we do not have a duty to monitor them to ensure that they are going to any specific place other than to check with our usual service providers that the withdrawal addresses in question are not ones that have been previously flagged as being part of any illicit activity. I can confirm that, in this case, there was no such confirmation. I say that this is our sole responsibility.

The complainant has not presented a positive case to show that there is any further duty of care and back this with any law or common law and, to that extent, we would say that there was nothing else that the service provider was required to do.

This is our evidence.'[16]

Complainant's representatives declined to cross-examine the evidence of the Service Provider.

Final Submissions

In their final submissions, the parties basically repeated what had already emerged in the Complaint, the Reply and the hearing proceedings.

Having heard the parties

Having seen all the documents

Considers

In failing to give proper evidence before the Arbiter and denying the Service Provider their right for a proper cross-examination of the case made in his Complaint, the Complainant has substantially prejudiced his case.

As the identity of the beneficial owners of the external wallets' recipients of the claimed fraudulent payments cannot be established, it was necessary to hear an emphatic negation from the Complainant that he himself was not a party to such

[16] P. 103 - 104

wallets. Such emphatic negation was only forthcoming from the side of the Service Provider.

Applicable Regulatory Framework

Foris DAX was, at the time of the events leading to this complaint, the holder of a Class 3 VFAA licence granted by the Malta Financial Services Authority ('MFSA') under the Virtual Financial Assets Act, 2018 ('VFAA').

Apart from the relevant provisions under the VFAA, and the *Virtual Financial Assets Regulations, 2018 (L.N. 357 of 2018)* issued under the same act, Foris DAX was also subject to the rules outlined in the Virtual Financial Assets Rulebook ('the VFA Rulebook') issued by the MFSA. The said rulebook complements the VFAA by detailing *inter alia* ongoing obligations applicable for VFA Service Providers.

Chapter 3 of the VFA Rulebook specifically includes the rules applicable for VFA Service Providers which such providers must adhere to.

The Arbiter further notes that in the year 2020, the MFSA has also issued a *'harmonised baseline guidance on Technology Arrangements'*[17] applicable to its licence holders (including under the Virtual Financial Assets) titled *'Guidance on Technology Arrangements, ICT and Security Risk Management, and Outsourcing Arrangements'* ('the Guidance').

Further Considerations

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

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

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

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

- The Complaint involves a series of payments made by the Complainant from his account held with Foris DAX, to 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 also given the nature of the transactions which involved crypto assets, the type of service provided, and other reasons as outlined below.

- The exchange of fiat currency into crypto and withdrawals from one's crypto account, including withdrawals to an external wallet is, in its own right, part of the typical services provided to millions of users by operators in the crypto field such as the Service Provider.

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

- The Complainant seems to have only contacted the Service Provider on 22 November 2023, some 4 months after the last of the disputed transactions was already executed and finalised.[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]

  Once a transaction is complete and, accordingly, is not in a pending state, the crypto transaction cannot be cancelled or reversed by the Service

[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

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 …'.[20]

On the basis of the facts presented during the case, the Arbiter could not conclude that the Service Provider failed to adhere to any specific obligation or any specific regulatory requirements applicable to it, nor did he find any infringement of the Terms and Conditions applicable in respect to the service offered.

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

i. 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

[20] P. 85
[21] https://fiaumalta.org/app/uploads/2020/09/20200918_IPsII_VFAs.pdf
[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'*

Laundering ('AML') and Combating of Financing of Terrorism ('CFT') obligations in terms of the local AML and CFT legislative framework.

Failures of the Service Provider in respect of AML/CFT are not in the remit of the OAFS and should be addressed to the FIAU. In the course of these procedures, no such failure was indeed alleged. In fact, it was declared that Boursorama, the French remitter bank, also made AML related enquiries with the Complainant and seemed satisfied with the outcome as they continued processing the payments. 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 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 largely happened in 2023.

The Arbiter shall thus not consider the MiCA provisions and Travel Rule obligations for the purposes of this Complaint.

iii. Othis - 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)*

[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

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 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. <u>Duty of Care and Fiduciary Obligations</u>

It is noted that Article 27 of the VFA Act states:

[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

[27] Such as Case ASF 069/2024

[28] Emphasis added by the Arbiter

'27. (1) Licence holders shall act honestly, fairly and professionally and shall comply with the requirements laid down in this Act and any regulations made and rules issued thereunder, as well as with other legal and regulatory requirements as may be applicable.

***(2) A licence holder shall be subject to fiduciary obligations as established in the Civil Code (CAP 16) in so far as applicable**.'*[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]

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:

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

"14. (1) A subject person having the control of assets belonging to a client shall safeguard such assets and the interest of the client therein.

…

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

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

No such out of norm event can be claimed during the short period of some two months when the fraudulent transfers were happening in relatively consistent quantity values in funds transferred from Complainant's account with his French Bank, Boursorama.

The Arbiter thus considers that the Service Provider did not breach, in terms of the provisions outlined in this decision, the duty of care and fiduciary obligations towards its customer, the Complainant, when considering the particular circumstances of this case.

Decision

It is clear that the Complainant has, unfortunately, fallen victim of a scam done by a third party and no evidence resulted that this third party is, in any way, related to the Service Provider.

Ultimately, the Arbiter does not consider that in the case in question, there is any clear and satisfactory evidence that has been brought forward, and/or emerged, during the proceedings of the case which could adequately corroborate that the Service Provider failed in any of the applicable obligations, contractually and/or arising from the VFA regulatory regime applicable in respect of its business.

The Arbiter notes that the crypto business is a relatively new area with no *harmonised regulation* existed at the time of the disputed transactions. An EU regulatory framework was only recently implemented effective for the first time in this field in 2025.[31]

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,[32] as translated into French legislation which, whilst applying to banks, are not applicable to VFA licensees.

The Arbiter notes that Complainant's representatives expressed intention to make similar claims for compensation from Boursorama on the basis that they had an obligation to intervene and stop Complainant from transferring his funds to a crypto exchange, given the much longer relationship between Complainant and his Bank permitting them to view in better context the abnormality of such payments.

A person who chooses to venture into the area of crypto which itself is typically a highly speculative and risky market, needs to also be highly conscious of the potential lack of, or lesser, consumer protection measures applicable to this area of business as compared to those found and expected in other established sectors of the financial services industry. EU regulatory bodies have issued various warnings to this effect over the past years.[33]

---

[31] 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/

[32] EU Directive 2015 - 2366

[33] https://www.eiopa.europa.eu/document-library/othis-documents/crypto-assets-esas-remind-consumers-about-risks_en

The Arbiter sympathises with the Complainant for the ordeal he may have suffered as a victim of a scam but, in the particular circumstances of this case, he cannot accept the Complainant's request for compensation for the reasons amply mentioned. The Arbiter is accordingly rejecting the Complaint.

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

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 on expiration of the period for appeal. Personal details of the Complainant(s) will be anonymised in terms of article 11(1)(f) of the Act.

https://www.esma.europa.eu/sites/default/files/library/esa_2022_15_joint_esas_warning_on_crypto-assets.pdf