Before the Arbiter for Financial Services

Case ASF 119/2025

TY

('the Complainant')

vs

Foris DAX MT Limited

(Reg. No. C88392)

('Foris' or 'the Service Provider')

Sitting of 13 March 2026

The Arbiter,

Having seen the Complaint made against Foris DAX MT Limited relating to its alleged failure to warn client that her transfer of digital assets (which digital assets were funded by transfer of Euro currency from her account with a bank in France known as N26 to her crypto account with Service Provider) to a fraudulent platform, has caused her a financial loss for which she is seeking compensation of €19,999.56[1].

The Complaint[2]

In her complaint form to the Office of the Arbiter for Financial Services ('OAFS'), the Complainant submitted that she was a victim of a cybercrime perpetrated by a fraudulent investment platform 'Smart Epargne' through *Crypto.com* whose misconduct allowed the fraudster operating the fraudulent platform to steal her money.

[1] Pages (p.). 3

[2] P. 1 - 6 with supporting documentation on P. 7 - 15.

She stated that she found the platform 'Smart Epargne' on the internet where it was positively introduced by a public figure. She searched that it was not a scam and clicked to make contact. Shortly after, she was contacted by a certain Philippe Leroux who introduced himself as a financial advisor and he guided her to make investments which later proved to be a fraud.

Three transfers were made as follows from her account with Crédit Mutuel to her account with N26.

Date	Amount €	Reference
03.01.2024	10,000	p. 60
06.01.2025	7,000	p. 60
08.01.2024	3,000	p. 60
Total	**20,000**	

These funds were then transferred from Bank N26 to the account of Foris (brand name Crypto.com) as follows:

Date	Amount €	Reference	Outward transfer to fraudster wallet
04.01.2024	2,000	p. 23	Changed to BTC 0.2428557 and transferred out same day
04.01.2024	8,000	p. 23	
09.01.2024	7000	p. 25	Changed to BTC 0.1610423 and transferred out same day
09.01.2024	3000	p. 26	Changed to BTC 0.0685175 and transferred out same day
Total	**20,000**		BTC 0.4706155 transferred out to wallet ending …6AZLL

Apart from the above reported fraudulent payments processed through Crypto.com APP, Complainant was seemingly also defrauded through other payments amounting to €999+€1050+€11,000+€4706=€17,775[3] which were sent to fraudsters using different channels.[4]

[3] Her total loss was accordingly €37,755 p. 60
[4] P. 60

These payments do not form part of this complaint which concern only payments and transfers processed through Foris.

It appears that the payments subject of this complaint were made for investment purposes which according to the fictitious website started generating profits. When Complainant wanted to cash out her profits, she was illuded to make the last payment of €4,706 as supposed tax due on the profits. When even this was not sufficient to encash her profits, Complainant finally realised she had been scammed.

She maintained that Service Provider should have detected the irregularity of the transactions on her account and should, at the very least, have questioned her and informed her of the potential suspicious nature of the transactions.[5]

It was claimed that Foris should have protected Complainant from sending her assets to the wallets controlled by the fraudsters and quoted various references to French law on this matter.[6]

Complainant denied she was guilty of negligence and explained that she had no intention of transferring her money for purposes other than investment and that the Service Provider (whom she addresses as Bank) failed to recognise the unusual nature of the transfers.[7] She then quotes various transaction monitoring obligations related to banks and finally concludes as follows:

'*In this case, [Complainant] intended to place her money securely. She simply followed the announced procedure to invest and subsequently to withdraw her funds without committing any fault.*

However, it was the fraudulent manoeuvres of the perperators that concealed the truth from [Complainant], hiding their real intentions.

The high level of fraud sophistication by the perpetrators, including the reproduction of professional-looking cryptocurrency trading platforms, persistent outreach, and customer support interactions during the withdrawal process, clearly contributed to the theft of [Complainant's] funds. Under these conditions, she could not have realised the deception. Furthermore, it should be

[5] P. 8 - 9
[6] Ibid.
[7] P. 9

noted that the fraud was carried out through methods of deceit and false appearance.

Consequently, you are obliged to reimburse the funds to the client, as she committed no fault.'[8]

Service Provider's reply

Having considered, in its entirety, the Service Provider's reply of 24 July 2025[9]

Where the Service Provider 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.*

    - *(The Complainant), e-mail address, xxxxx@hotmail.fr, became a customer of Foris DAX MT Limited through the Crypto.com App and was approved to use the Wallet on 3 January 2024.*

    - *The Company notes that in the submitted complaints file, the Complainant's representative has outlined the desired remedy as: (i) reimbursement for incurred financial losses*.'[10]

The Service Provider then provided a timeline for the transactions explained above which resulted in BTC 0.4706155 being transferred out to wallet ending … 6AZLL which was controlled by the fraudsters.

[8] P.10
[9] P. 22 - 30 with attachments from p. 31 - 38
[10] P. 22

They further submitted as follows:

'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 herself.

While we sympathize with the Complainant and recognize that she may have been misled or induced into transferring funds to an alleged fraudster, it is important to note that these transfers were made solely at the Complainant's request. We must also emphasize that the address the funds were transferred to does not belong to the Company and as such, any due diligence of the ownership of this address falls under the responsibilities of the provider of said wallet.

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

The Complainant is solely responsible for the security and authenticity of all instructions submitted through 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 its sole discretion that the transaction should be cancelled or reversed and is technically capable of such cancellation or reversal. You acknowledge that you are responsible for ensuring the accuracy of any instructions submitted to Crypto.com and that any errors may result in the irreversible loss of your Digital Asset.

…

Service Provider's Warnings

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

The first of these warnings appear whenever a user adds a new withdrawal address to the Cryto.com App. For the reference of the Tribunal, the warning appears a below, in Fig. 12. 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. 13.

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. 14 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 Wallet, 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 Wallet.

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

Summary

In summary, it seems conceivable that the Complainant has been the victim of an alleged scam. However, due to the nature of the external wallet and the fact that it is not hosted or operated by 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 she had willingly, transferred her virtual asset holdings from her Crypto.com Wallet to an external wallet address which she 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. 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 hearing of 25 November 2025, the Complainant failed to make presence and was represented by his French counsel who largely restated the contents of the filed complaint.

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

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

Complainant's lawyers assented to such ruling and confirmed that the transfers in question were concluded with the full authority of Complainant.

The Complainant's legal representative stated:

'We understand that under the law, any financial services or cryptocurrency exchanges company is required to differentiate between two types of clients.

First, an uninformed person, generally, an individual, qualifies for the bank's duty to warn.

Second, an informed person, generally, a professional, is presumed to know the risks associated with investment operations. And, in principle, the payer bears all losses resulting from unauthorised payment operations if their losses arise from fraudulent conduct on their part, or intentionally, or with gross negligence, fail to comply with their obligations.

[11] P. 27 - 30

And so, these obligations are taking all reasonable measures to preserve the security of personalised security data, promptly informing the payment service provider of any misappropriation of funds and blocking fraudulent payments.

So, this is not the case here, but [Complainant] committed no error.

Moreover, she did not disclose any personal data to third parties and, consequently, Crypto is required to return the funds to the client as she committed no fault."[12]

The Arbiter explained that as Complainant has accepted that she had personally authorised the transfers subject of this complaint,[13] the issue of not being at fault because she did not disclose her secret credentials is irrelevant. The relevant issue is whether the Service Provider could or should have done anything, according to law and regulations, to identify the fraud and stop the payments in spite of their being fully authorised.

At the hearing, the Arbiter requested the Complainant's representative to file a translated copy of the fraud report made to the French Authorities and of the complaint filed on her French Bank, if applicable. Complainant's legal representative informed that they had received compensation from Crédit Mutuel for the payments made through channels other than Crypto.com but the Arbiter wanted to see the complaint against N26 that was the remitter bank of the transfers made to Crypto.com.[14]

A translated copy of a report dated 15 September 2024 filed with the French Public Prosector was submitted.[15]

A second hearing was held on 12 January 2026, and this was attended by the Complainant who confirmed all the information her legal representative had given at the previous hearing and declared she had nothing else to say.

The legal representative of Foris requested a copy of the mediation decision which resulted in a partial recovery from Crédit Mutuel, but Arbiter stated that as this concerns recovery of payments not part of this complaint, he does not compel the Complainant to provide it.

[12] P. 42
[13] P. 43
[14] P. 53 - 58
[15] P. 59 - 78

The legal representative of Complainant informed there were no developments on the complaint filed on N26.

Pema Fung then submitted evidence on behalf of the Service Provider where she stated:

'The Complainant became a client and user of the Service Provider on the 3rd of January 2024.

The disputed transactions in question relate to three withdrawals of Bitcoin cryptocurrency, which were purchased in the Complainant's Crypto.com app account and sent to one single external wallet address between the 4th and the 9th of January 2024.

This wallet address is what we call a non-custodial address, which means that they are not serviced by Crypto.com or identified from the data on the blockchain as serviced by a similar exchange, like the Service Provider.

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

With regard to warnings, in the course of the Complainant's disputed transactions, the Service Provider had provided numerous warnings regarding withdrawals to the external wallets, which has been already detailed in the Service Provider's original reply, and this will not be repeated here.

The Service Provider would also like to highlight here that it is in the evidence of the Complainant in the letter from Ziegler entitled 'Formal Notice' and dated 15th September 2024, that the Complainant was fully aware of the dangers of scams. In fact, the third paragraph of this letter mentions the fact that the Complainant did some research into the trading platform, followed by the fourth paragraph of this letter, which states that the Complainant, I quote,

'Wanting to make sure it wasn't a scam, [Complainant] continued her research. Finding no negative information online, [Complainant] decided to invest.'

In spite of the Complainant's own awareness of the existence and dangers of scams, and the numerous warnings mentioned by the Service Provider at the

whitelisting and withdrawal stages, the Complainant proceeded to make the withdrawals to the external wallets whilst negligently disregarding the warnings.

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

In so far that the transactions have been completed to the full satisfaction of what we were asked to execute on behalf of the Complainant, the Service Provider does not bear any responsibility for the loss in regard to these transactions.'[16]

There was no cross examination of Ms Fung's evidence by the legal representative of the Complainant.

Final Submissions

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

Complainant explained that as the mediation proceedings held with Crédit Mutuel were subject to confidentiality conditions which prevent them submitting documentary evidence, they confirm that a settlement of €3,150 was made as partial compensation for the loss suffered.[17]

However, this referred to settlement of claims which are totally different from the payments covered by this complaint (as above explained).

The final submissions of the Service Provider were based on the incorrect assumption that the Complainant had failed to attend the last hearing of 12 January 2026.[18] This is false as Complainant attended and was available for cross-examination.

[16] P. 82 -83
[17] P. 88
[18] P. 90 - 92 points 5 - 12

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.

The Arbiter further notes that in the year 2020, the MFSA has also issued a *'harmonised baseline guidance on Technology Arrangements'*[19] applicable to its licence holders (including under the Virtual Financial Assets) titled *'Guidance on Technology Arrangements, ICT and Security Risk Management, and Outsourcing Arrangements'* ('the Guidance').

Further Considerations

Having considered the particular circumstances of the case including the submissions made and evidence provided, the Arbiter considers that 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 herself transferred to an external wallet from her crypto account.

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

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

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 her account held with Foris DAX to an unknown external wallet.

  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, 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 her crypto.

- The Complainant seems to have only contacted the Service Provider on 15 September 2024[20] almost 9 months after the last of the disputed transactions was already executed and finalised.[21]

[20] P. 7 - 10 Foris maintain this was only received on 03.01.2025 p. 79

[21] 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).

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).[22]

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 …'.[23]

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. <u>AML/CFT Framework</u>

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'*.[24]

These are *'sector-specific Implementing Procedures [which] complement the Implementing Procedures – Part I [issued by FIAU] and are to be read in*

[22] E.G. https://www.chargebackgurus.com/blog/chargebacks-more-volatile-complex-than-cryptocurrency
[23] P. 83
[24] https://fiaumalta.org/app/uploads/2020/09/20200918_IPsII_VFAs.pdf

conjunction therewith'.[25] Section 2.3 of these Implementing Procedures detail the monitoring and transaction records obligations of VFA licensed entities.

It is noted that the VFA Act mainly imposes transaction monitoring obligations on the Service Provider for the proper execution of their duties for Anti-Money Laundering ('AML') and Combating of Financing of Terrorism ('CFT') obligations in terms of the local AML and CFT legislative framework.

Failures of the Service Provider in respect of AML/CFT are not in the remit of the OAFS and should be addressed to the FIAU. In the course of these procedures, no such failure was indeed alleged. The Arbiter shall accordingly not consider compliance or otherwise with AML/CFT obligations in this case.

ii. MiCA and the Travel Rule

As to the identification of the recipient of the funds, it is noted that MiCA[26] and Travel Rule[27] obligations which entered into force in 2025 and which give more protection to consumers by having more transparency of the owners of the recipient wallets were not applicable at the time of the events covered in this Complaint which happened in 2024. 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)*

[25] Page 6 of the FIAU's Implementing Procedures on the *'Application of Anti-Money Laundering and Countering the Funding of Terrorism Obligations to the Virtual Financial Assets Sector'*

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

[27] EU Directive 2023/1113 https://eur-lex.europa.eu/legal-content/AUTO/?uri=CELEX:32023R1113&qid=1740401464257&rid=1 and EBA Guidelines on Travel Rule https://www.eba.europa.eu/sites/default/files/2024-07/6de6e9b9-0ed9-49cd-985d-c0834b5b4356/Travel%20Rule%20Guidelines.pdf

VASPs should be aware that with the coming into force of Regulation (EU) 2023/1113 and the Travel Rule Guidelines[28] their obligation to have reliable records on the owners of external (unhosted) wallets increases exponentially as from 30 December 2024.

Arguments that they have no means of knowing who are the owners of external wallets which have been whitelisted for payments by their client will lose their force.

VASPs have been long encouraged by the Office of the Arbiter (in decisions dating back from 2022),[29] for the devise of enhanced mechanisms to mitigate the occurrence of customers falling victims to such scams.

Furthermore, in the Arbiter's decisions of recent months there is a recommendation that VASPs should enhance their on-boarding processes where retail customers are concerned warning them that custodial wallets may be used by scammers promoting get-rich-quick schemes as a route to empty the bank accounts of retail customers and disappear such funds in the complex web of blockchain anonymous transactions.[30]

***Compliance with such recommendations or lack thereof will be taken into consideration in future complaint adjudications**."[31]*

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

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:

[28] *Guidelines on information requirements in relation to transfers of funds and certain crypto-assets transfers under Regulation (EU) 2023/1113* - EBA/GL/2024/11 of 04/07/2024
https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32023R1113
https://www.eba.europa.eu/publications-and-media/press-releases/eba-issues-travel-rule-guidance-tackle-money-laundering-and-terrorist-financing-transfers-funds-and

[29] Such as Case ASF 158/2021

[30] Such as Case ASF 069/2024

[31] Emphasis added by the Arbiter

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

***(2) A licence holder shall be subject to fiduciary obligations as established in the Civil Code (CAP 16) in so far as applicable**."*[32]

Article 1124A (1)(a) of the Civil Code (Chapter 16 of the Laws of Malta), in turn further provides the following:

"1124A. (1) ***Fiduciary obligations arise in virtue of law, contract, quasi-contract****, unilateral declarations including wills, trusts,* ***assumption of office or behaviour whenever a person*** *(the ''fiduciary'') –*

(a) ***owes a duty to protect the interests of another person and it shall be presumed that such an obligation where a fiduciary acts in or occupies a position of trust is in favour of another person****;…"*[33]

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

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

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:

[32] Emphasis added by the Arbiter
[33] 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 just over one month when the fraudulent transfers were happening in relatively consistent quantity values in funds transferred from Complainant's account with her French Bank.

The Arbiter when considering the particular circumstances of this case, 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.

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.

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* 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.[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. 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 her complaint, the Complainant refers to provisions of the PSD 2,[35] as translated into French legislation, which whilst applying to Banks are not applicable to VFA licensees. She also often wrongly addresses Foris as a bank/neo bank, which clearly, they are not.

The Arbiter was informed that similar claims for compensation was made on Complaint's French Bank on the basis that they had an obligation to intervene and stop Complainant from transferring her funds to a crypto exchange, given the much longer relationship between Complainant and her Bank permitting them to view in better context the claimed 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.[36]

---

[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/

[35] EU Directive 2015 - 2366

[36] 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 she may have suffered as a victim of a scam but, in the 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.

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

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.