Before the Arbiter for Financial Services

Case ASF 108/2025

FO

('the Complainant')

vs

Foris DAX MT Limited

(Reg. No. C 88392)

('Foris' or 'Service Provider')

Sitting of 6 February 2026

The Arbiter,

Having seen the Complaint made against Foris DAX MT Limited relating to its alleged failure to warn client that his transfer of digital assets (which digital assets were funded by transfer of Euro currency from his bank account with Crédit Agricole (France) to his account with Service Provider) to a fraudulent platform, has caused him a financial loss for which he is seeking compensation of €9,600.77.[1]

The Complaint[2]

In his complaint form to the Office of the Arbiter for Financial Services ('OAFS'), the Complainant submitted that he was a victim of a cybercrime perpetrated by a fraudulent person who called herself Grace Collins who presented herself as an experienced crypto currency trading expert and introduced him to the ZipCoinEx platform.

[1] Page (p.) 3

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

From a copy of the report made by Complainant to the Frech Public Prosecutor,[3] it appears that the loss subject matter of this complaint was preceded by 5 other payments amounting to €78,000 from his accounts with Alpha Bank and Crédit Agricole to accounts he appears to have held with different crypto exchanges (Coin Base and Binance).

The payments related to the Complaint were specifically made from Crédit Agricole on 27 September 2024 to his account with Crypto.com (which is the brand name of Foris) which is acknowledged as received in Foris's reply for €9.600.[4]

There seems to be some confusion on the total extent of the loss suffered by the Complainant. The report to the Public Prosector above referred to speaks of a total loss of €77,648 whereas the total payments listed amount to €87,600, being €78,000 (5 payments prior) and the Complaint amount of €9,600.

It is quite possible that the difference is explained by withdrawals allowed by scammers to enhance their credibility.

Be as it may, this case involves a single payment of €9,600 as above explained.

In his complaint, he stated that:

"*On August 27, 2024, (the Complainant) successfully made his first withdrawal of 5,900 USDT, followed by a second withdrawal of 1,720 USDT on September 8, 2024, which further reassured him about the platform's reliability. However, by the end of September, ZipCoinEx suddenly demanded repayment of a 70,000 USDT credit without allowing him to use his profits to cover this obligation.*

Under pressure, (the Complainant) transferred an additional €10,000 and borrowed 0.22 BTC from Mr xxxxx, a friend, hoping to continue his trading activities.

On September 27, 2024, during a new trading session, (the Complainant) recorded profits of 17,518 USDT and 55,130 USDT. Ms Collins informed him that a final session would occur on October 2, 2024, after which he could withdraw all his funds. This last session resulted in an additional gain of 107,800 USDT.

[3] P. 42 - 49
[4] P. 25

However, on October 3, 2024, when attempting to withdraw 30,000 USDT, the ZipCoinEx platform blocked the transaction, citing a security verification process. The following day, Ms Collins required him to complete his identification by providing a copy of his driver's licence, which he did. Subsequently, the platform imposed a security deposit of $70,000 (15% of his holdings) to unlock his funds. He was given a seven-day deadline to make this payment with the threat that his funds would otherwise be frozen for 180 days."[5]

He maintains that Service Provider should have detected the irregularity of the transactions on his account and, therefore, held them responsible for the loss.

He claims that Foris should have protected him from sending his assets to the wallets controlled by the fraudsters and quoted various references to French law on this matter.[6]

Complainant denied he was guilty of negligence and explained that he had no intention of transferring his money for purposes other than investment and the Service Provider (whom he at times refers to as a bank) failed to note the unusual nature of the transfers and failed its duty of vigilance as it never contacted Complainant to flag the transaction and enquire its purpose.[7] He then quotes various transaction monitoring obligations related to banks and finally concludes as follows:

> *"In this case, (Complainant) made no mistake. He did not disclose any personal data to third parties. Consequently, (Service Provider) must return the funds to the client, as the latter committed no fault".*[8]

Service Provider's reply

Having considered in its entirety the Service Provider's reply,[9]

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

[5] P. 4
[6] P. 9 - 12
[7] P. 11
[8] P. 12
[9] P. 24 - 28 with attachments from p. 29 - 34.

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@gmail.com, became a customer of Foris DAX MT Limited through the Crypto.com App and was approved to use the Wallet on 26 September 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 of the Complainant's account with them for the above-mentioned inward transfer of Euro fiat currency. These funds were then converted to crypto assets and transferred out to an external wallet.

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

[10] P. 24

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:

"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 appears whenever a user adds a new withdrawal address to the Cryto.com App. For the reference of the Tribunal, the warning appears a below, in Fig. 5. 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. 6.

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. 7 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 the Company, we can neither confirm nor deny this.

Whilst we fully empathize with the Complainant in this regard, it cannot be overlooked that they had willingly, transferred their virtual asset holdings from their Crypto.com Wallet to external wallet addresses which they 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

For the first hearing on 29 September 2025, the Complainant failed to make presence and was represented by his French counsel.

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.

[11] P. 26 - 28

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 need only 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 ruling and confirmed that the payment was made with full authority of the Complainant.[12]

At the hearing, the Arbiter requested the Complainant's representative to file a copy of the fraud report made to the French Authorities and to inform whether a complaint was filed against his home bank.

A copy of the report dated 11 November 2024 made to French Authorities was sent following the first hearing.[13] A copy of the claim against Crédit Agricole dated 6 December 2025 was also submitted.[14]

A second hearing was held on 24 November 2025 for the evidence of the Service Provider. As Complainant was present for the second hearing, he was given the opportunity to confirm all that his legal representative had stated on his behalf at the first hearing. He re-confirmed that the payment was duly authorised by him and that he had nothing to add.

The legal representative of the Service Provider queried the date of 6 December 2025 (p. 51) of the report made to Crédit Agricole which is a future date attached to an email dated 10 October 2025 (p. 41).

The legal representative of Complainant explained that the original report was sent in February 2025, and it was rejected in April 2025. The matter was then referred to the mediator of the French Banking Federation in June, and they are still awaiting a reply. The legal representative stated that the date of 6 December 2025 is not correct.[15]

[12] P. 38
[13] P. 42 - 50
[14] P. 51 - 60
[15] P. 63 - 65

The Service Provider then proceeded with their evidence and stated:

"***The complainant became a client and user of the service provider on the 26th of September 2024. The disputed transaction in question relates to the withdrawal of cryptocurrency which was purchased on the Crypto.com app and sent to one wallet address on the 27th of September, 2024.***

The wallet address is what we call a non-custodial address, which means they are not serviced by Crypto.com or identified as from the data on the blockchain provided by service providers in similar sphere.

From the evidence at hand and the agreement of the complainant's legal representative and his confirmation today, this transaction was fully authorised by him. At the time of the withdrawal, the address wallet in question was not subject to any warnings from our own internal investigations or any third-party transaction monitoring tools that we use.

Furthermore, in the course of the disputed transaction, the service provider had provided numerous warnings regarding withdrawals to the external wallet. The first of these warnings would have appeared when the complainant added a new withdrawal address to the Crypto.com app called whitelisting. And this takes the form of a full screen pop-up. A similar warning would appear during the withdrawal stage to the withdrawal address which had already been whitelisted on the previous occasion. Both pop-up warnings specifically warned the complainant against scams and to not 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 the withdrawal, the complainant was 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 would have taken him to the regularly updated Crypto.com Help Centre Page called, 'Avoiding Digital Currency Scams'.

Upon the complainant confirming that he had read the scam warning by clicking on 'Confirm and withdrawal' button on the pop-up warning, the complainant confirmed that he had accepted the risks involved and took full responsibility for the withdrawals to the external wallet, specifically agreeing

to and acknowledging that the withdrawal was irreversible and that the service provider would not be liable for assets sent to the external wallet. In spite of these warnings mentioned, the complainant proceeded to make the withdrawal to the external wallet. It can be seen that the complainant acted negligently by disregarding these warnings.

It is noted that the screenshots of these warnings have not been included in the service provider's reply. Should Mr. Arbiter require this evidence, we will be happy to include it after the close of today's hearings.

Lastly, we would like to stress that nothing in our controls as well as the controls of our third-party employed tools indicate that there was any malicious or scam activity involved in the case at the time it happened.

We were not communicated with or brought to the attention of the complainant's concerns with this transaction until after the transaction had already been completed. Therefore, 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, we would say that the service provider bears no responsibility with regard to the transaction involved."[16]

Complainant's representative did not cross-examine the evidence but demanded evidence of the warnings given to Complainant mentioned in the evidence of the Service Provider. These were submitted after the second hearing.[17]

Final Submissions

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

However, the Service Provider's assertions that the Complainant was not available to give live evidence and for cross-examination[18] is incorrect as such facility was available at the second hearing as above explained.

[16] P. 63 - 65
[17] P. 67 - 71
[18] P. 78

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

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

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 payment made by the Complainant from his 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 involve 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 disputed transaction was already executed and finalised.[20]

  Once finalised, the crypto cannot be cancelled or reversed as specified in the Service Provider's Terms and Conditions of Use (and as typically indicated on various other internet sites).[21]

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

[20] Crypto transactions may be processed and completed within a few minutes or hours (as indicated on various websites following a general search on the internet).
[21] E.G. https://www.chargebackgurus.com/blog/chargebacks-more-volatile-complex-than-cryptocurrency

Provider as provided for and warned in the Terms and Conditions of Foris DAX.

As indicated by the Service Provider, Clause 7.2(b) of its Terms and Conditions regarding the use of the Crypto.com App Services specifies that:

'Crypto.com processes all Digital Asset Transfers according to the Instructions received from you and does not guarantee the identity of any recipient. You should verify all transaction information prior to submitting Instructions for a Digital Asset Transfer to Crypto.com as the Digital Asset Transfer may not be cancelled or reversed once processed …'.[22]

Based on the facts presented during the case, the Arbiter could not conclude that 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'*.

These are *'sector-specific Implementing Procedures [which] complement the Implementing Procedures – Part I [issued by FIAU] and are to be read in conjunction therewith'*.[23] Section 2.3 of these Implementing Procedures detail the monitoring and transaction records obligations of VFA licensed entities.

It is noted that the VFA Act mainly imposes transaction monitoring obligations on the Service Provider for the proper execution of their duties for Anti Money

[22] P. 27

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

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[24] and Travel Rule[25] obligations which entered into force in 2025 and which give more protection to consumers by having more transparency of the owners of the recipient wallets were not applicable at the time of the events covered in this Complaint which happened in 2023. The Arbiter shall thus not consider the MiCA provisions and Travel Rule obligations for the purposes of this Complaint.

iii. Other - Technical Note

A Technical Note (issued in 2025) with guidance on complaints related to pig butchering was recently published by the Arbiter. In respect of VFA licensees, the Technical Note states as follows:

> *"Virtual Financial Assets Service Providers (VASPs)*
>
> *VASPs should be aware that with the coming into force of Regulation (EU) 2023/1113 and the Travel Rule Guidelines[26] their obligation to have reliable records on the owners of external (unhosted) wallets increases exponentially as from 30 December 2024.*

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

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

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

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

VASPs have been long encouraged by the Office of the Arbiter (in decisions dating back from 2022),[27] for the devise of enhanced mechanisms to mitigate the occurrence of customers falling victims to such scams.

Furthermore, in the Arbiter's decisions of recent months there is a recommendation that VASPs should enhance their on-boarding processes where retail customers are concerned warning them that custodial wallets may be used by scammers promoting get-rich-quick schemes as a route to empty the bank accounts of retail customers and disappear such funds in the complex web of blockchain anonymous transactions.[28]

***Compliance with such recommendations or lack thereof will be taken into consideration in future complaint adjudications**."*[29]

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

Hence, for the avoidance of any doubt, the said Technical Note is not applicable to the case in question.

iv. Duty of Care and Fiduciary Obligations

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

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

***(2) A licence holder shall be subject to fiduciary obligations as established in the Civil Code (CAP 16) in so far as applicable**."*[30]

[27] Such as Case ASF 158/2021
[28] Such as Case ASF 069/2024
[29] Emphasis added by the Arbiter
[30] Emphasis added by the Arbiter

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

> *"1124A. (1)* ***Fiduciary obligations arise in virtue of law, contract, quasi-contract****, unilateral declarations including wills, trusts,* ***assumption of office or behaviour whenever a person*** *(the ''fiduciary'') –*
>
> *(a)* ***owes a duty to protect the interests of another person and it shall be presumed that such an obligation where a fiduciary acts in or occupies a position of trust is in favour of another person****; …".*[31]

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

[31] Emphasis added by the Arbiter

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 nothing which is out the ordinary to a degree which should have triggered the application of the fiduciary duties of the Service Provider. The complaint involves a single payment made just after the account relationship was established and an authorised transfer to an external wallet of crypto assets immediately after the received funds were exchanged.

There were no payment patterns which could have given rise to reasonable suspicion of fraud, and Complainant was clearly warned, as was prudent, to ensure that he knows and has confidence in the beneficiaries of the external wallet.

Decision

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

The Arbiter notes that the crypto business is a relatively new area with no *harmonised regulation* existing at the time of the disputed transactions. An EU regulatory framework was only recently implemented effective for the first time in this field in 2025.[32]

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

[32] Provisional agreement has been reached on the EU's Markets in Crypto-Assets Regulation (MiCA) only in June 2022 - https://www.consilium.europa.eu/en/press/press-releases/2022/06/30/digital-finance-agreement-reached-on-european-crypto-assets-regulation-mica/
MiCA entered into force in 2025 – https://www.financemagnates.com/cryptocurrency/can-mica-take-europe-to-the-crypto-promised-land/

a certain amount of security to the consumer, since they are still relatively in their infancy, may not necessarily reflect the same standards and protections applicable in other sectors of the financial services industry which have long been regulated.

In fact, the Arbiter notes that in his complaint, the Complainant refers to provisions of the PSD 2,[33] as translated into French legislation, which whilst applying to Banks are not applicable to VFA licensees. He also at times wrongly addresses Foris as a bank which clearly, they are not.

A person who chooses to venture into the area of crypto which, itself, is typically a highly speculative and risky market, needs to also be highly conscious of the potential lack of, or lesser, consumer protection measures applicable to this area of business as compared to those found and expected in other established sectors of the financial services industry. EU regulatory bodies have issued various warnings to this effect over the past years.[34]

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 that Service Provider has failed in their regulatory and fiduciary obligations.

Consequently, 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

[33] EU Directive 2015 - 2366
[34] https://www.eiopa.europa.eu/document-library/othis-documents/crypto-assets-esas-remind-consumers-about-risks_en
https://www.esma.europa.eu/sites/default/files/library/esa_2022_15_joint_esas_warning_on_crypto-assets.pdf

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.