**Before the Arbiter for Financial Services**

**Case ASF 078/2025**

**WE**

**('the Complainant')**

**vs**

**Foris DAX MT Limited**

**(Reg. No. C88392)**

**('Foris' or**

**'Service Provider')**

**Sitting of 21 May 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 Banque Dupey de Parseval to his account with Service Provider) to a fraudulent platform, has caused him a financial loss for which he is seeking compensation of €825,066[1].

Following clarification sought in the first hearing of 22 September 2025,[2] it was confirmed by the lawyers of the Complainant that the amount indicated in the complaint is the total loss suffered from this fraud experience but the Complaint involving the Service Provider is limited to four payments listed below

[1] Page (p.) 4
[2] P. 82 - 83

amounting to €246,500. Accordingly, the amount claimed under this complaint was reduced to €246,500.

**The Complaint**[3]

In his complaint form to the Office of the Arbiter for Financial Services ('OAFS'), the Complainant submitted that he was a victim of a cybercrime perpetrated by fraudulent persons who purported to be representatives of STIGMA-FINANCE investment platform on which he registered on 08 April 2024 to subscribe to an alleged algorithm managed investment fund title 'Formule Plenitude' requiring a base capital of €760,000.

He claims that in total he invested €246,500 through 4 transactions as shown in the Table below which were credited to his account with the Service Provider that was opened on 23 February 2024.

| Sequence number | Date | Amount in EURO | Received by Service Provider |
|---|---|---|---|
| 1 | 28.02.2024 | 30,000 | p. 34 |
| 2 | 29.02.2024 | 28,500 | p. 35 |
| 3 | 08.03.2024 | 50,000 | p. 36 |
| 4 | 25.03.2024 | 138,000 | p. 37 |
| | | | |
| As per complaint as revised | **Total** | **246,500** | |

The Complaint also explains that following these payments, the Complainant continued to make other 'investments' in 2024. He mentions 9 other payments effected between 30 April 2024 and 29 May 2024 amounting to an additional

[3] P. 1 - 7 with supporting documentation on P. 8 - 58.

€576,566[4] which were sent to the fraudulent investments platform through other channels and which are not included in this Complaint against Foris.

From the reply of Foris referred to hereunder it results that each of these funds transfer was immediately converted to crypto assets and transferred to 2 external wallets ending …. *xtZ5V and …. ee7d2* so that by the end of the process, the Complainant had transferred 1.342131374 BTC (Bitcoin) and 11.32582215 ETH (Ethereum) between 01 March 2024 and 26 March 2024[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 gross negligence as he had not disclosed any personal data to third parties[7]. He then quotes various transaction monitoring obligations related to banks and finally concludes as follows:

> *"In this case, (Complainant) did not make any errors. He did not disclose any personal data to third parties. Consequently, the financial institution, Crypto.com, must reimburse the funds to (Complainant) as the latter committed no wrongdoing."*[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:

[4] P. 3
[5] P. 70
[6] P. 9 - 12
[7] P. 12
[8] P. ibid
[9] P. 65 - 72 with attachments from p. 73 - 81

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 xxxx@bbox.fr, became a customer of Foris DAX MT Limited through the Crypto.com App and was approved to use the Wallet on 23 February 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. These included above-listed inward transfers of Euro fiat currency. These funds were then converted to crypto assets (BTC and ETH) and transferred out to the external wallet as above referred to.

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. 65

*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:*

*QUOTE*

*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.*

*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 external wallet addresses which he nominated.*

*As outlined above in the Foris DAX MT Limited Terms of Use, the Complainant is solely responsible for the security and authenticity of all instructions submitted through the Crypto.com App and, as such, the Company cannot accept liability for the veracity of any third party or for the instructions received from the Complainant themselves."*[11]

**Hearings**

For the first hearing on 22 September 2025, the Complainant failed to make presence and was represented by his French counsel. The hearing was dedicated to clarification of the amount of compensation sought as above described.[12]

At the second hearing held on 25 November 2025, the Complainant again failed to make presence, and the meeting was postponed with a clear warning that any further failure in this regard will lead to abandonment and closure of the case without adjudication.

The Arbiter asked for submission by Complainant of a translated copy of the report of the scam filed with French Authorities[13] and claim on French bank that remitted the funds to Complainant's account with Foris (Crypto.com).

[11] P. 71 - 72
[12] P. 82 - 91
[13] P. 96 - 104

For the third hearing held on 13 February 2026, the Complainant was present assisted by a translator and his French Lawyer, Mr. Alexandre Dakos.

On being cross-examined he stated:

***"It is said that in my complaint, I refer to a contractual arrangement, correspondence exchanged mentioning a base capital with Stigma-Finance.***

***Asked whether in my contractual arrangements and all the correspondence I had with Stigma-Finance, Crypto.com was involved in that correspondence; whether I was a party to that contract and whether Crypto.com was also part of this advice with the financial analyst, I say that there is a contract signed only with Stigma-Finance who asked me to open an account with Crypto.com. The contract was also made with Kraken.***

***Asked whether it is correct to say that all this correspondence with the financial analyst was just between me and these individuals indicated in the complaint, such as Mr Fontaine, and not with Crypto.com, I say that it was not only with the analysts but also with people from Crypto.com and Kraken in order to open the accounts.***

***Asked whether between 28 February 2024 and May 2024, when these transactions were being conducted, I sought advice from anyone else, such as a financial advisor or someone regulated to give advice on this contract or on these transactions, I say, yes. They advised me on how to invest in Bitcoins.***

***Asked who are 'they', I say that at the beginning, it was Mr Barbier, and then when they said they fired him, Mr Fontaine came and started to advise me. I say, yes, they were from Stigma-Finance.***

***It is said that it seems that the last transaction from the complaint was made on 29 May 2024. Yet I wrote to Crypto on 28 December 2024, (page 15 of the complaint file.)***

***Asked why it took me from May until December to write to Crypto asking for a refund of these transactions, I say that it took me time to finalise the transfer that was requested and I had to take loans from my loved ones. When I figured out what happened, I went to the law firm in June 2025, and then it took time for them to go to the bank and make the complaint. In France, justice is really***

***slow. That is why it took so much time. I say that I started the procedures in June.***

***Asked whether I filed a complaint with Banque Dupuy De Parseval, I say, yes.***

***Asked when this was filed and whether there is any outcome from those proceedings, I say that I made the complaint in June 2025 and we had the response from the mediator of the bank at the start of December 2025.***

***Asked what the mediator decided, I say that they refused my demand because they were not in agreement with what had been said. They are proceeding with the procedure and have sent their response; we are waiting for the final response. I say that the mediator was not in agreement because he stated that the bank warned me of the risks, but I say that this is not true because they did not tell me about the risks of the transactions. So, we are waiting for a final answer now.***

***I am asked whether the other parties could have a copy of this mediation, as this is an important factor to this complaint; if they could have evidence of the claim made against the bank, the reply, and any new action taken.***

***The Arbiter intervenes to request an explanation from Mr Dakos whether they can have a copy of these because he had already asked for these in the past.***

***Mr Alexandre Dakos replies:***

***The reason why we did not give it to you is because in France, the French mediation procedure is strictly confidential, and we are not allowed to give copies of it to anybody else.***

***The Arbiter accepts this because mediation is confidential in the OAFS's proceedings as well. And once the mediation is unsuccessful, then it is regarded as if it did not happen.***

***The Arbiter understands that the Complainant is taking more action against the bank because he is not happy with the mediation.***

***Asked whether this is correct, the Complainant replies:***

***Yes, it is correct. Indeed, there is no judicial action being taken, but we contest the first response of the mediation. We are waiting for the response."***[14]

**….**

***"I am asked whether when making these payments, which are quite substantial—especially the payment of €138,000—the bank asked me what this was or what I was doing, and whether they, in any way, tried to convince me or asked questions about my payments.***

***I say that the bank never alerted me to any risks regarding these payments. That were being made to open an account with Crypto.com.***

**Cross-examination continues:**

***"It is said that these transactions from 28 February until 22 March were all authorised by me, that I made these transactions.***

***Asked whether this is correct, I say, yes. I made them with my money, but Stigma-Finance asked me to make them.***

***Asked when I was conducting these transactions, whether I remember receiving any warnings or pop-up warnings from Crypto.com in my app or on the device I was using; whether I remember being asked to make sure that I was not sending this money to a fraudulent account and to read more if I wanted more information prior to transacting, I say, no, never.***

***I confirm that I am an architect, an established architect by profession.***

***So, asked whether, when I was entering into these agreements and facilitating these transactions of quite a substantial amount, I did not think it prudent to seek advice from a third party, my bank, or a licensed financial advisor before entering into all these transactions and contracts, I say, yes.***

***I asked around, but because I exchanged a lot with Stigma analysts and they were contacting me constantly every day, we started to have a very close relationship and almost a friendship. The arguments were so good that I trusted them.***

[14] P. 105 - 107

***It is said that the link between me and Crypto.com is simply that the money was transferred from my personal bank account to the wallet indicated by Stigma; that it was just used as a transfer. That there was no history with Crypto; I did not use Crypto as a platform before. That it was simply a platform to transfer the money from my bank account to this wallet indicated by Stigma.***

***Asked whether this is correct, I say that historically there was no link with Crypto.com, but I was very new and we had exchanges by email about the transactions and they answered when I made the transfers."***[15]

A fourth hearing was held on 12 March 2026, for the evidence of the Service Provider where Pema Fund stated:

***"The Complainant became a client of the Service Provider on the 23rd of February 2024.***

***The disputed transactions in question relate to withdrawals of Bitcoin cryptocurrency which was purchased in the Complainant's Crypto.com app account to two external wallet addresses between the 1st and 26th of March 2024.***

***These wallet addresses are what we call non-custodial addresses, which means that they are not serviced by Crypto.com or identified from data on the blockchain as being serviced by a similar company or exchange.***

***We have evidence before us that these transactions were fully authorised by the Complainant and made pursuant to his instructions.***

***The Service Provider would like to highlight that we have no affiliation whatsoever with Stigma Finance or with the individuals referred to in the complaint, namely, Mr. Fontaine and Mr. Barbier.***

***There is also no historical relationship between the Complainant and the Service Provider prior to this incident. The Complainant entered into a contractual relationship with the third-party scammers in which Crypto.com, the Service Provider, had no involvement.***

[15] P. 108 - 109

***In the course of the Complainant's disputed transactions, the Service Provider had provided numerous warnings regarding withdrawals to the external wallets.***

***The first of these warnings appeared at the whitelisting process when a user added a new withdrawal address to the Crypto.com app. This 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 is being made to an address that has already been whitelisted on a 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, or to people the Complainant did not know well, and to any source the Complainant did not have complete confidence in.***

***In addition, the Complainant is further warned that the withdrawal is irreversible and is also encouraged to learn more about safety and protection from scams by clicking the link 'Learn More' that is available in the pop-up button.***

***Upon the Complainant confirming that they had read the scam warning by clicking on the confirm and withdraw button on the pop-up warning, the Complainant confirmed they accepted the risks involved and took full responsibility for the withdrawals to the external wallets, specifically agreeing to and acknowledging that the withdrawals were irreversible and that the Service Provider would not be liable for assets sent to external wallets.***

***In spite of the numerous warnings mentioned above provided by the Service Provider, the Complainant proceeded to make the withdrawals to the external wallets whilst negligently disregarding these warnings.***

***Lastly, there is nothing in our own controls as well as the controls of our third-party monitoring tools to indicate that there is 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 after these transactions had already been completed.***

***Thank you. Insofar 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 regarding any of these transactions."***[16]

Invited to cross-examine, the lawyer of the Complainant opted not to.

The Arbiter requested copies of warnings referred to in Service Provider's evidence[17] and a copy of KYC documents when onboarding the Complainant[18].

**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**

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.

[16] P. 111 - 113
[17] P. 115 - 120
[18] P. 121

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.

The Arbiter further considers various factors, including, the nature of the complaint, activities involved, and the alleged shortfalls as further detailed below:

- The Complaint involves a series of payments made by the Complainant from his account held with Foris DAX, to unknown external wallets.

  The Arbiter considers that **except as deliberated hereunder under Fiduciary Duty obligations**, no adequate and sufficient evidence has however emerged to substantiate the claim that the Service Provider could have itself prevented or stopped the transaction. This is also given the nature of the transactions which involved crypto assets, the type of service provided, and other reasons as outlined below.

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

- Furthermore, it has not been demonstrated nor emerged that the alleged fraudster, to whom the payment was made by the Complainant, was another *Crypto.com* App user and, thus, a client of the Service Provider in the first place. The transfer was rather indicated to have been done to an

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

*'external wallet'* and hence the Service Provider had no information about the third party to whom the Complainant was transferring his crypto.

- The Complainant seems to have only contacted the Service Provider well after the last of the disputed transactions was already executed and finalised.[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 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, **except as treated hereunder under the Fiduciary Duty obligations**, 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:

[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
[22] P. 71 - 72

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'*.[23]

These are *'sector-specific Implementing Procedures [which] complement the Implementing Procedures – Part I [issued by FIAU] and are to be read in conjunction therewith'*.[24] Section 2.3 of these Implementing Procedures detail the monitoring and transaction records obligations of VFA licensed entities.

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

Failures of the Service Provider in respect of AML/CFT are not in the remit of the OAFS and should be addressed to the FIAU. The Arbiter shall accordingly not consider compliance or otherwise with AML/CFT obligations in this case.

ii. MiCA and the Travel Rule

As to the identification of the recipient of the funds, it is noted that MiCA[25] and Travel Rule[26] 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.

[23] P. 101 - 102

[24] 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'*

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

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

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

iii. Other - Technical Note

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

> *"Virtual Financial Assets Service Providers (VASPs)*
>
> *VASPs should be aware that with the coming into force of Regulation (EU) 2023/1113 and the Travel Rule Guidelines[27] 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),[28] 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.[29]*
>
> ***Compliance with such recommendations or lack thereof will be taken into consideration in future complaint adjudications**."[30]*

[27] *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

[28] Such as Case ASF 158/2021

[29] Such as Case ASF 069/2024

[30] Emphasis added by the Arbiter

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**."*[31]

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**;…"*[32]

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:

[31] Emphasis added by the Arbiter
[32] Emphasis added by the Arbiter

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

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

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

*…*

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

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

In the particular circumstances of this case, there is an event which is out the ordinary to a degree which should have triggered the application of the fiduciary duties of the Service Provider, in particular:

1. KYC documents[33] provided by the Service Provider consisted merely of proof of identification. The obligation regarding KYC goes beyond mere identification.

[33] P. 121

2. In similar cases against the same Service Provider, they presented a questionnaire where customer indicated his range of annual income and the turnover he expects to put through his account. In this case no such information was provided.

3. Accordingly, the Service Provider had no benchmark to judge the turnover of nearly quarter of a million Euro in less than one month on Complainant's account.

4. The Arbiter is of the opinion that when processing the last payment of 25 March 2024 for €138,000, the Service Provider should have taken steps to fill the KYC gaps before proceeding, even though there is no claim or suspicion that Service Provider failed to ensure the clean provenance of the funds.

For sake of clarity, the Arbiter explains that whilst he is not the competent authority to investigate breaches related to AML/CFT obligations as earlier explained in this decision, he is competent to investigate whether in the process of performing such obligations, the Service Provider failed in its fiduciary duty to warn its customers of reasonable suspicion of fraud/scams emerging in the process of conducting its regulatory duties.

The Arbiter, when considering the particular circumstances of this case, considers that for reasons explained above the Service Provider breached the duty of care and fiduciary obligations towards its customer, the Complainant. For this purpose, a copy of this decision is being sent to the Malta Financial Services Authority (Malta Regulator of CASPs) for their consideration of any regulatory action they may consider appropriate.

**Decision**

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

The Arbiter notes that the crypto business is a relatively new area with no *harmonised regulation* existed at the time of the disputed transactions. An EU

regulatory framework was only recently implemented effective for the first time in this field in 2025.[34]

Whilst this area of business had remained unregulated in certain jurisdictions, other jurisdictions, like Malta, chose to regulate this field in the meantime and subject it to a home-grown national regulatory regime. 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,[35] 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.[36]

In deciding what compensation, if any, would be appropriate in the particular circumstances of this case the Arbiter has to consider whether the breach of fiduciary duty as above explained was the cause of the loss suffered by the Complainant and whether there are any other factors which are more dominant contributors to such loss.

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

The Arbiter considers that there could be other dominant causes for this loss, namely:

1. The Complainant's gross negligence and greed in making investments expecting quick high returns[37] without taking any advice or precautions[38].

2. The obligation of the home bank to spot the fraud and issue timely warning to Complainant.

The obligations of fiduciary duty and transaction monitoring apply more forcefully to licensed banks than they apply to CASPs/VFA agents. Banks have a much longer relationship with their clients, and they have the data to spot unusual transactions and suspect fraud. On the other hand, customer's relationship with a VFA is short without much historical data to enable early spotting of unusual patterns of payments.

Banks can only avoid, under the provisions of PSD 2, to reimburse fraud payments even if authenticated and authorised by their client, if the client has shown gross negligence in the process.

In terms of preamble 71 of the said PSD2[39], the PSU (Complainant) shall be responsible for payment of any unauthorised payment transaction only up to a limit of €50, unless the PSU has acted fraudulently or with gross negligence.

---

[37] P. 9 speaks of request to pay €186,543 being 2% flat tax supposedly negotiated with FCA. This represents profits of some €9.3 million on which 2% flat tax would explain the amount of payment requested by the fraudsters to pay such 'tax' as a pre-condition to releasing the profits.

[38] P. 109 ***"I did not think it prudent to seek advice from a third party, my bank, or a licensed financial advisor before entering into all these transactions and contracts"***

[39] Preamble 71 of PSD 2 (**DIRECTIVE (EU) 2015/2366)** states**:**

*"In the case of an unauthorised payment transaction, the payment service provider should immediately refund the amount of that transaction to the payer. However, where there is a high suspicion of an unauthorised transaction resulting from fraudulent behaviour by the payment service user and where that suspicion is based on objective grounds which are communicated to the relevant national authority, the payment service provider should be able to conduct, within a reasonable time, an investigation before refunding the payer. In order to protect the payer from any disadvantages, the credit value date of the refund should not be later than the date when the amount has been debited. In order to provide an incentive for the payment service user to notify, without undue delay, the payment service provider of any theft or loss of a payment instrument and thus to reduce the risk of unauthorised payment transactions, the user should be liable only for a very limited amount**, ***unless the payment service user has acted fraudulently or with gross negligence****. In that context, an amount of EUR 50 seems to be adequate in order to ensure a harmonised and high-level user protection within the Union. There should be no liability where the payer is not in a position to become aware of the loss, theft or misappropriation of the payment instrument. Moreover, once users have notified a payment service provider that their payment instrument may have been compromised, payment service users should not be required to*

In the absence of gross negligence, there could well be an obligation on the part of the home bank to make quasi-total refunds to their client (Complainant). The banks' obligation for effective transaction monitoring are direct and specific under the EU Directive PSD 2. On the other hand, the transaction monitoring obligations on CASP/VFA result only from general fiduciary duties and are less direct and forceful than those applicable to banks.

If reimbursement of losses is denied by the home bank on the basis of gross negligence on the part of the Complainant, the same gross negligence would exempt Foris from being a clear direct cause of his claimed losses.

**The Arbiter sympathises with the Complainant for the ordeal he may have suffered as a victim of a scam but, in the particular circumstances of this case, he cannot accept the Complainant's request for compensation as he has failed to provide any evidence of direct causation of the breaches of fiduciary duties to the loss incurred[40].**

**In the absence of such evidence, there is risk that other parties are found potentially primarily responsible for this loss, so that if the Arbiter were to award any compensation without full information on the responsibility of other actors in the fraud journey, this could lead to undue enrichment.**

**The Complainant denies that he has received any warnings from his French Bank. However, he has failed to provide copies of his complaint to his Bank and has been quite evasive on the proceedings going on to force such claim. The Arbiter deems it possible that the home bank could have warned Complainant on the risk of fraud during the payments journey and that their warnings were ignored in a manner that could prove gross negligence on the part of Complainant.**

*cover any further losses stemming from unauthorised use of that instrument. This Directive should be without prejudice to payment service providers' responsibility for technical security of their own products."* ( emphasis added by Arbiter)

[40] This line of reasoning was included in decision AFS 042/2024, which decision was confirmed by Court of Appeal (inferior jurisdiction) case ref 35/2025 file:///C:/Users/mifsa208/Downloads/28_01_2026-35_2025-158407%20(1).pdf

**For the above reasons, this Complaint is not upheld, and no compensation is being ordered.**

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

**Alfred Mifsud**
**Arbiter for Financial Services**

**Information Note related to the Arbiter's decision**

*Right of Appeal*

The Arbiter's Decision is legally binding on the parties, subject only to the right of an appeal regulated by article 27 of the Arbiter for Financial Services Act (Cap. 555) ('the Act') to the Court of Appeal (Inferior Jurisdiction), not later than twenty (20) days from the date of notification of the Decision or, in the event of a request for clarification or correction of the Decision requested in terms of article 26(4) of the Act, from the date of notification of such interpretation or clarification or correction as provided for under article 27(3) of the Act.

Any requests for clarification of the award or requests to correct any errors in computation or clerical or typographical or similar errors requested in terms of article 26(4) of the Act, are to be filed with the Arbiter, with a copy to the other party, within fifteen (15) days from notification of the Decision in terms of the said article.

In accordance with established practice, the Arbiter's Decision will be uploaded on the OAFS website. Personal details of the Complainant(s) will be anonymised in terms of article 11(1)(f) of the Act.