Before the Arbiter for Financial Services

Case ASF 106/2025

ID

('the Complainant')

vs

Foris DAX MT Limited

(Reg. No. C 88392)

('Foris' or 'the 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 account with Crédit Agricole bank in France to his crypto account with Service Provider) to a fraudulent platform, has caused him a financial loss for which he is seeking compensation of €97,549.83[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 investment platform, 'HighBTCStock', through *Crypto.com* whose misconduct allowed the fraudster operating the fraudulent platform to steal his money. He claims that it all started in October 2023 when he was offered attractive investment proposals ranging from €10,000 to €100,000 with possibility to borrow against such funds from the platform.

He stated:

[1] Pages (p.). 4

[2] P. 1 - 8 with supporting documentation on P. 9 - 84.

'Ultimately, following the instructions of this supposed trader, [the Complainant] installed several applications, including AnyDesk, Crypto.com, and Coinbase Wallet, enabling cryptocurrency fund management, and made fund transfers according to the following circuit: the transfers were initiated from his bank account held at Crédit Agricole to his Crypto.com account. These funds were then transferred to Coinbase Wallet before being ultimately directed to the HighBTCStock platform as follows:'

He reported the following payments were made to his account with Crypto.com (brand name of Foris):

Date	**Amount € rounded**	**Reference to Foris's reply**
27.10.2023	4,950	€5,000, p. 91
23.11.2023	9,000	2 transfers €4,000 + €5,000, p.92
17.04.2023	1,999	€2,000 p. 93
24.04.2024	6,001	3 transfers €2,000 x 3, p.94
29.05.2024	2,600	€2,700, p. 95
16.10.2024	6,000	3 transfers €2,000 x 3, p.96 - 97
22.10.2024	6,750	3 transfers €2,300; €2,000; €2,500, p.97-98
29.10.2024	6,700	3 transfers €2,100; €2,000; €2,500, p.98-99
07.11.2024	10,000	5 transfers €2,500 x 2; €2,000 x 2; €1,000, p.100
07.11.2024	280	6 transfers totalling €16,400: 2500+3000+1000+3500+3500+3000 p. 101 - 104
07.11.2024	2,500	
07.11.2024	3,700	
08.11.2024	10,000	
13.11.2024	13,500	p. 105
29.11.2024	2,070	p. 106
29.11.2024	2,000	p.107
29.11.2024	2,000	p. 108
29.11.2024	7,500	p. 109
TOTAL	**97,550**	

Complainant declared that in September 2024, he requested a withdrawal of €30,000 as his investments were showing a balance of USDC[3] 313,027. Scammers demanded a payment of 3.5% tax and 10% of profits made amounting to USDC 28,000. Somehow, a purported digital wallet holder, Coinbase, got involved requesting tax payments and fees of US$6565 and, finally, Coinbase confirmed on 15.11.2024 that all taxes had been paid but they could not effect any transfer as HighBTCStock imposed a restriction.

On 20 November 2024, Complainant was informed by AMF (French Financial Regulator) that HighBTCStock was on its blacklist and advised him to secure his Coinbase wallet.

It is not clear why Complainant continued to make payments on 20.11.2024 after being so informed on the 20.11.2024, but it is probable that he was dealing with a fake Coinbase so much so that after demanding return of USDC 189,580 not blocked by HighBTCStock, he was contacted by the latter demanding a further 10% commission before releasing the Coinbase hold.

At this stage, Complainant realised he was the victim of a scam and filed a report with the French Police on 30.11.2024.

It was claimed that Foris should have protected Complainant from sending his assets to the wallets controlled by the fraudsters and quoted various references to French law on this matter.[4]

Complainant denied he was guilty of negligence and explained that he had no intention of transferring his money for purposes other than investment. He claimed that the Service Provider (whom he addresses as Bank) failed to note the unusual nature of the transfers.[5]

He then quotes various transaction monitoring obligations related to banks and finally concludes as follows:

> *'In this case, (Complainant) made no error. He did not disclose any personal data to third parties.*
>
> *As a result, (Service Provider) must return the funds to the client, as the latter has committed no wrongdoing.'*[6]

[3] USDC is a digital stable coin linked 1:1 with US$
[4] P. 12 - 14
[5] P. 13
[6] P. 14

Service Provider's reply

Having considered in its entirety, the Service Provider's reply,[7]

Where the Service Provider provided a summary of the events which preceded the Complainant's formal complaint and explained and 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@gmail.com, became a customer of Foris DAX MT Limited through the Crypto.com App and was approved to use the Wallet on 20 October 2023.*
- *The Company notes that in the submitted complaints file, the Complainant's representative has outlined the desired remedy as: (i) reimbursement for incurred financial losses*."[8]

The Service Provider then provided a timeline for the transactions of the Complainant's account with them. These consisted of the above listed inward transfers of Euro fiat currency collectively amounting to circa €97,500 as shown in the Table above. These funds were then converted to crypto assets (BTC and ETH) and the transferred through several transactions totalling BTC 0.54603321 an ETH 27.34654 to 8 external wallets.[9]

Foris submitted that:

[7] P. 90 - 112 with attachments from p.113 - 143.
[8] P. 90
[9] P. 109

'*For the avoidance of doubt, the External Wallets are not serviced by the Service Provider and accordingly, the Service Provider does not have any information pertaining to the owner(s) of them.*

Service Provider's Internal Investigation

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 External Wallets the funds were transferred to, do not belong to the Company and as such, any due diligence of the ownership of these addresses falls under the responsibilities of the provider of the External 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 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. 78. 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. 79.

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. 80 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 Wallets, 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 Wallets.

In spite of the numerous warnings mentioned above, the Complainant proceeded to make the withdrawals to the External Wallets. 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 he had willingly transferred his virtual asset holdings from his Crypto.com Wallet to external wallet addresses which he nominated.

As outlined above in the Foris DAX MT Limited Terms of Use and as accepted pursuant to each withdrawal warning, the Complainant is solely responsible for the security and authenticity of all instructions submitted through the Crypto.com App and, as such, the Company cannot accept liability for the veracity of any third party or for the instructions received from the Complainant themselves. This is particularly emphasized against the backdrop of each warning that the Complainant has received upon every whitelisting and withdrawal transaction."[10]

Hearings

[10] P. 110 - 112

During the hearings, the Complainant failed to make presence and was represented by his French counsel who largely re-stated 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 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 whilst Service Provider wished to register the following statement:

'***The service provider submits that the absence of the complainant renders, obviously, cross-examination impossible.***

As has been reiterated before, cross-examination is a fundamental principle in testing the credibility and reliability of the evidence, and is essential in the proper administration of justice.

Without the opportunity to cross-examine the complainant, Foris DAX is denied a fair opportunity to challenge the case against them.

Foris DAX submits that the complainant's absence is not only procedurally unfair, but results in unnecessary time and costs being incurred by the defendant who has attended in good faith to answer the allegations.

On this point, I would just like to say that Foris DAX, because of the repeated absence of the complainants, reserves its right to proceed for the unnecessary delay, the wasted time, the avoidable legal costs which the service provider is incurring, because, once again, the service provider has always been present in attendance, and has engaged in these contentious proceedings in good faith.

I am not asking any questions to the representative of the complainant because it is all hearsay.'[11]

[11] P. 146

The Arbiter explained that as Complainant has accepted that he had personally authorised the transfers subject of this complaint[12], the issue of not being at fault because he did not disclose his 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,[13] and a copy of any claim made against the French remitter bank claiming their failure to alert Complainant under their transaction monitoring obligations.[14]

At the second hearing (where Complainant again failed to make presence) held on 24 November 2025, the Arbiter made the following declaration:

'***The Arbiter states that this is the second hearing of this case. The Arbiter has received the documents he requested at the last hearing of 29 September 2025.***

The Arbiter states that from the police report, the total sum of the scam is €97,549 which is the exact amount listed in the complaint. However, in the claim against Crédit Agricole, dated 17 March 2025, the amount claimed from the bank is €114,227.

The Arbiter states that there is a difference of about €16,000 and if the Arbiter understands correctly, the difference is made up of some card payments listed at the top of page 171 which is €20,000 less some recoveries referred making the net amount to €16,000.

Since the amount in the police report matches the amount in the complaint, the Arbiter concludes that the letter to Crédit Agricole includes about €16,000 additional payments which were not part of the complaint and not part of the police report.

Ms Roskach replies that she has to ask Mr Alexandre Dakos for this information.

The Arbiter is going on with the amount claimed of €97,000.'[15]

[12] P. 146
[13] p. 151 - 167 report to Pubic Prosector which refers to a police report filed on 30.11.2024
[14] P. 168 - 182 claiming total damages amounting to €114,227.25
[15] P. 183

When asked to update the hearing on any progress and on state of affairs of the case opened against Crédit Agricole (remitter bank), the legal representative of the Complainant said she had no information about the matter.

The Arbiter noted the statement but warned the legal representative that she should be better prepared for the hearings especially in the failed presence of the Complainant. After making enquiries with her colleagues, she reported that:

'***I have no questions for Ms Fung but would like to answer the questions that the Service Provider had asked earlier.***

As regard to the complaint, the criminal investigation is still ongoing.

As regard to the formal notice, we were rejected by Crédit Agricole bank. So, we have referred the matter to the mediator and we are currently awaiting their response.'[16]

The Arbiter stated that in the absence of any evidence to the contrary, he has to assume that Crédit Agricole, in terms of the provisions of PSD2,[17]could only have denied the claim as they upheld that the loss was caused by the Complainant's gross negligence.[18]

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

The evidence of the Service Provider was conducted by Pema Fung who stated:

'***The complainant became a client and user of the service provider on the 20th of October 2023. The disputed transactions in question relate to the withdrawals of cryptocurrency which were purchased on the Crypto.com app and sent to eight different wallet address between 27th of October 2023 to 29th of November 2024.***

These wallet addresses are what we call non-custodial addresses, which are not serviced by Crypto.com or identified as from the data on the blockchain provided by service providers of similar nature.

From the evidence at hand and the agreement of the complainant's legal representatives, these transactions were fully authorised by the complainant.

[16] P. 186
[17] EU Directive 2023/1113
[18] Preamble 71 of the PSD2 EU Directive 2023/1113

At the time of the withdrawals, none of these address wallets in question were subject to any warnings from our own internal investigations or any third-party transaction monitoring tools that we use.

Furthermore, there were multiple warnings to the complainant during the course of the disputed transactions. 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 at the time of each withdrawal whether or not the withdrawal address had been newly whitelisted or had already been in use 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, 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 withdrawals, 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 take users to the regularly updated Crypto.com help center page called, 'Avoiding Digital Currency Scams.'.

Upon the complainant confirming that he had read the scam warnings 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 wallets, 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 wallets. In spite of the numerous warnings mentioned above, the complainant proceeded to make the withdrawals to these external wallets. 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 in the note of final submissions or after the close of today's hearings.

Lastly, we would like to stress again that nothing in our own controls as well as the controls of our third-party employed tools indicated 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 these transactions until after the transactions 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 these disputed transactions.'[19]

There was no cross examination of evidence by the legal representative of the Complainant.

After the hearing, the Service Provider sent as requested copies of the warnings given to Complainant at the time of whitelisting a new external wallet and prior to effecting any transfer to such wallet.[20]

Final Submissions

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

Having heard the parties

Having seen all the documents

Considers

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

As the identity of the beneficial owners of the external wallets' recipients of the claimed fraudulent payments cannot be established, it was necessary to hear an emphatic negation from the Complainant that he was a party to such wallets. Such emphatic negation was only forthcoming from the side of the Service Provider.

[19] P. 185 - 186
[20] P. 193 - 197

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'*[21] applicable to its licence holders (including under the Virtual Financial Assets) titled *'Guidance on Technology Arrangements, ICT and Security Risk Management, and Outsourcing Arrangements'* ('the Guidance').

Further Considerations

Having considered the particular circumstances of the case, including the submissions made and evidence provided, the Arbiter considers that there is no sufficient and adequate basis on which he can uphold the Complainant's request for the reimbursement by the Service Provider of the sum the Complainant himself transferred to an external wallet from his crypto account. At no stage has the Complainant raised any doubt as to his 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 his account held with Foris DAX to an unknown external wallet.

[21] 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 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, in its own right, part of the typical services provided to millions of users by operators in the crypto field such as the Service Provider.

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

- The Complainant seems to have only contacted the Service Provider in March 2025[22] more than 3 months after the last of the disputed transactions was already executed and finalised.[23]

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).[24]

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

[22] P. 16

[23] 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).

[24] E.G. https://www.chargebackgurus.com/blog/chargebacks-more-volatile-complex-than-cryptocurrency

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 …'.[25]

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

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

i. AML/CFT Framework

Further to the Prevention of Money Laundering Act (Cap. 373) and Prevention of Money Laundering and Funding of Terrorism Regulations ('PMLFTR'), the Financial Intelligence Analysis Unit (FIAU) issued Implementing Procedures including on the *'Application of Anti-Money Laundering and Countering the Funding of Terrorism Obligations to the Virtual Financial Assets Sector'*.[26]

These are *'sector-specific Implementing Procedures [which] complement the Implementing Procedures – Part I [issued by FIAU] and are to be read in conjunction therewith'*.[27] 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.

[25] P. 111
[26] https://fiaumalta.org/app/uploads/2020/09/20200918_IPsII_VFAs.pdf
[27] 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'*

ii. MiCA and the Travel Rule

As to the identification of the recipient of the funds, it is noted that MiCA[28] and Travel Rule[29] 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)*
>
> *VASPs should be aware that with the coming into force of Regulation (EU) 2023/1113 and the Travel Rule Guidelines[30] 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),[31] 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 onboarding processes where retail customers are concerned warning them that custodial wallets*

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

[29] 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

[30] *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

[31] Such as Case ASF 158/2021

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.[32]

***Compliance with such recommendations or lack thereof will be taken into consideration in future complaint adjudications**."*[33]

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**."*[34]

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**; …"*[35]

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

[32] Such as Case ASF 069/2024
[33] Emphasis added by the Arbiter
[34] Emphasis added by the Arbiter
[35] Emphasis added by the Arbiter

applied to the Service Provider at the time of the disputed transactions in 2022, provides that:

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

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

> *"14. (1) A subject person having the control of assets belonging to a client shall safeguard such assets and the interest of the client therein.*
>
> *…*
>
> *(7) The subject person shall make appropriate arrangements for the protection of clients' assets held under control and shall ensure that such assets are placed under adequate systems to safeguard such assets from damage, misappropriation or other loss and which permit the delivery of such assets only in accordance with the terms and conditions of the agreement entered into with the client."*

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

No such out of norm event can be claimed during the short period of just over one year when the fraudulent transfers were happening in relatively consistent quantity values in funds transferred from Complainant's account with his French Bank. There was no particular transfer for any out of pattern amount which would have alerted the Service Provider to suspect fraud and raise the matter with Complainant.

The highest single transfer was for an amount of €13,500 on 13.11.2024 which was only slightly above other payments received in a fragmented manner on same day as explained in the Table above.

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

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

The Arbiter notes that the crypto business is a relatively new area with no *harmonised regulation* 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.[36]

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 Complaint refers to provisions of the PSD 2,[37] as translated into French legislation which whilst applying to Banks, are not applicable to VFA licensees. He also often wrongly addresses Foris as a 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

[36] 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/

[37] EU Directive 2015 - 2366

and stop Complainant from transferring his funds to a crypto exchange, given the much longer relationship between Complainant and his Bank permitting them to view in better context the claimed abnormality of such payments.

The fact that the French Bank (with whom Complainant has much longer relationship than he had with the Service Provider) has denied responsibility on the basis of gross negligence on the part of the Complainant, indicates that not even the French Bank has accepted any responsibility for any failure in their transaction monitoring systems and obligations. This notwithstanding that PSD 2 places much stricter obligations for transaction monitoring on licensed credit institution (banks) than on VFA agents who are only bound by general fiduciary duties.

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.[38]

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

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

However, the Arbiter warns that for new complaints registered after September 2025, in cases where the Complainants fail to attend hearings to defend their complaint without valid reasons, they will be obliged to settle the fees of the respondent Service Providers.

Alfred Mifsud
Arbiter for Financial Services

[38] 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.