Before the Arbiter for Financial Services

Case ASF 011/2025

JH

('the Complainant')

vs

Foris DAX MT Limited (C 88392)

('Foris' or 'the Service Provider')

Sitting of 31 October 2025

The Arbiter,

Having seen the **Complaint** dated 13 January 2025[1] relating to the Service Provider's alleged failure to prevent, stop or reverse the payment in crypto of Bitcoin (BTC) made by the Complainant herself from her account held with *Crypto.com* to two external wallets allegedly owned by third parties who could be fraudsters or connected to fraudsters.

The Complaint

The Complainant opened an account with the Service Provider in September 2024.

Between 17 and 26 September 2024, she funded her account with three transfers for a total value of €32,000 carried out by multiple transactions involving exchanging such funds to BTC followed by prompt transfers of such BTC to external wallets which later turned out to be controlled by scammers.

[1] Pages (p.) 1 - 8 and attachments p. 9 - 34

Complainant at the time believed that the BTC were being transferred to her investment portfolio on a platform Entrust Capital Ltd (https//entrustcapltd.com)

On each occasion, the funds were immediately converted to BTC and transferred out to the external wallets.

The following Table gives details of these transfers:

Date	Transfers in Euro	Remitter Bank	Exchanged to BTC net of charges	Date transferred to scam wallet
17.09.2024	7000	Revolut[2]	0.1268989	18.09.2024[3]
25.09.2024	2000	Kantonalbank[4]	0.4218	26.09.2024 via 3 transfers[5]
25.09.2024	23000	Kantonalbank[6]		
Total	**32000**		**0.5486989**[7]	

The Complainant stated that:

"From August 13, 2024, to October 17, 2024, I was under severe pressure from professional fraudsters. They frequently called me, using different numbers, and convinced me to share my phone screen. I had never used the screen-sharing function before and was unaware of the existence. Under their dictation and constant pressure, I performed all the actions they instructed me to do.

The fraudsters convinced me to transfer funds to their platform Entrust Capital Ltd (https://entrustcapital.com). Initially, I used my bank card for these transfers. Later, they told me that to continue investing, I need to open an account on

[2] P. 16
[3] P. 44
[4] P. 18
[5] P. 45 - 46
[6] P. 20
[7] P. 46

Crypto.com. They explained that this was necessary for handling larger amounts and assured me that it was important for successful investments.

I completely relied on their instructions as I was not familiar with cryptocurrency. I do not speak English, and I had no understanding of the process. The fraudsters guided me step by step in opening an account on Crypto.com, dictating what to press while I shared my phone screen. Afterward, they provided me with IBAN numbers and explained that I needed to transfer money 'to my profile' on the Entrust Capital platform. I did not realise that these transfers were processed through cryptocurrency and that the funds were ultimately directed to Crypto.com.

When the fraudsters decided that the Crypto.com account was no longer needed, they once again guided my actions, and under their supervision, I deleted the account.

Details of the Situation

1. *Efforts to Understand the Situation: After realising I was a victim of fraud, I contacted Aargauische Kantonalbank and other banks to investigate the IBAN numbers used for the transfers. I believed I was transferring money to regular bank accounts and did not understand that these were intermediaries. These inquiries yielded no results as the banks could not find any information.*

2. *Communication with Crypto.com Support: Simultaneously, I contacted Crypto.com support online to request transaction records. However, I did not receive a response – I was repeatedly told that the request was 'being processed'. This continued for about three weeks, and I began to doubt that Crypto.com was willing to help. As I was waiting for these transaction records, my police report was delayed. My mental state worsened, and I began to suspect that Crypto.com might be connected to the fraudsters, as they kept evading my request.*

3. *Email Communication: When online support did not provide an answer, I found an alternative email contact, db@crypto.com (or another, if needed), and sent a request for the transaction details. I was informed that they*

could only provide the transactions via an official request from law enforcement, and that only the police could obtain access to these records.

4. *Filing a Police Report: After receiving no transaction details from Crypto.com, I filed a report with the local police in Switzerland without these transactions. I do not know the status of the investigation, as no one has communicated with me about it. I also filed a report with Action Fraud in the United Kingdom in October, as the fraudsters claimed their company Entrust Capital Fraud had branches in the UK and Dubai. Later, I also filed a report with the police in Dubai. All this information will be provided upon request.*

5. *Mental and Emotional State: This situation has caused severe stress and panic attacks. I am under psychiatric care. My hospitalisation was scheduled for December 11, 2024, but I was forced to delay it until December 23, as I have no one to care for my child, and I cannot afford a nanny. The fraudsters not only manipulated me but continued calling from different numbers, even after I blocked them on messaging platforms. These calls persisted, exacerbating my condition.*

6. *Communication with MFSA and Other Authorities: I also reached out to the Malta Financial Services Authority (MFSA) and other financial institutions to obtain information about intermediaries like PayNome (Finance Incorporated Limited) and how they are connected to Crypto.com. Although, I attempted to gather information, I was not provided with the necessary details. It was only later that I learned that the funds were connected to Crypto.,com.*

My Request

1. *I request a full investigation into the transactions and to identify the final recipient of the funds.*

2. *I urge you to ensure that Crypto.com cooperates not only with law enforcement but also directly with me, the affected customer.*

3. *I request the full refund of the funds transferred to the fraudsters through Crypto.com, as I was manipulated under duress and did not fully understand the nature of the transactions."*[8]

Reply of Service Provider[9]

In their reply of 06 March 2025, Service Provider explained that Foris offers the following services:

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@hotmail.ch, became a customer of Foris DAX MT Limited through the Crypto.com App and was approved to use the Wallet on 27 September 2024.*
- *The Company notes that in the submitted complaints file, the Complainant has outlined her desired remedy as: (i) reimbursement for incurred financial losses.*[10]

They gave a detailed sequence of the various transactions executed by the Complainant on her Wallet.[11]

They concluded that:

[8] P. 3 - 5
[9] P. 43 - 47 and attachments p. 48 - 52
[10] P. 43
[11] P. 44 - 46

"Based on our investigation, the Company has concluded that we are unable to honor the Complainant's refund request based on the fact that the reported transfers were made by the Complainant herself.

While we sympathize with the Complainant and recognize that she may have been misled or induced into transferring funds to an alleged fraudster, it is important to note that these transfers were made solely at the Complainant's request. We must also emphasize that the addresses the funds were transferred to, do not belong to the Company and as such, any due diligence of the ownership of these addresses falls under the responsibilities of the provider of said 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 her Wallet as outlined in the Foris DAX MT Limited Terms of Use.

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

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 she had willingly transferred her virtual asset holdings from her Crypto.com Wallet to external wallet addresses which she nominated.

As outlined above in the Foris DAX MT Limited Terms of Use, the Complainant is solely responsible for the security and authenticity of all instructions submitted through the Crypto.com App and, as such, the Company cannot accept liability for the veracity of any third party or for the instructions received from the Complainant themselves."[12]

Contumacy

As the reply of the Service Provider was received later than the 20 days allowed by law (Article 22(3)(c) of the Act Chapter 555), the Arbiter had to consider whether to apply contumacy rules to Foris.

The Arbiter's recent decisions on contumacy issues contained guidance on the application of contumacy in cases presented for his adjudication:

1. Contumacy will apply if Arbiter is convinced that the delay was meant to be disrespectful of his and his Office role.
2. Chapter 555 does not oblige the Arbiter to enforce contumacy where this would go against the provisions to deal with complains in a procedurally fair, informal, economical and expeditious manner in terms of Article 19(3)(d).
3. Article 19(3)(b) of Chapter 555 obliges the Arbiter to adjudicate complaints by reference to what, in his opinion, is fair, equitable and reasonable in the particular circumstances of the case.
4. Arbiter feels that the duty to hear both sides of the complaint with equal opportunities is superior to technical inhibitions that may apply in Court

[12] P. 46 - 47

but require more liberal interpretation in Arbitration obliged to procedures of informality.

For these reasons, the Arbiter will apply contumacy only in cases where:

a. There is clear evidence of disrespect towards the Arbiter or his Office;

   or

b. Service Provider not only replies late (or does not reply) but fails to be present for the first hearing;

   or

c. Service Provider's reply is registered late in a manner which the Arbiter considers exaggerated.

In view of the above, the Arbiter decided not to apply contumacy rules against Foris.

Hearings

During the first hearing held on 17 July 2025, Complainant largely repeated what she had stated in her complaint, but she added that before the transfers subject of this complaint, Service Provider had stopped a similar transaction and, therefore, could not understand why having stopped one transaction they let subsequent transactions go through leading to realisation of the scam.

Whilst admitting that she had authorised the transfer to Entrust Capital, she could not explain why some payments were blocked by Crypto.com whilst others were allowed to pass.

She also stated under cross-examination:

"Asked since I wanted to continue to invest in Entrust Capital, and I decided to invest larger amounts of money, whether I asked, checked or verified about Entrust Capital Limited, whether I asked my bank if it was a legitimated account or whether I checked on Google, I say that I checked on the internet and I found that this company exists with offices in London and Dubai. That this company is licensed in Dubai.

… …

Asked by the Arbiter whether the Complainant opened this account on the instructions given to her by the fraudsters, the Complainant replied, 'Yes'.

Asked by the Arbiter whether the Complainant authorised the transfers herself to the wallet which we now know belonged to the fraudsters on the instructions of the fraudsters, the Complainant replied that she authorised the transfers herself and saw her money on the account of Entrust Capital."[13]

Following the first hearing, the Complainant sent an email dated 19 June 2025 wherein she elaborated:

1. ***"One transaction was unexpectedly cancelled in the Crypto.com app***

   While making transfers through the Crypto.com application, one of the transactions was unexpectedly cancelled, while all subsequent ones were processed without issue.

   Please take into account why this particular transaction was blocked – was it perhaps flagged by the system as suspicious? If so, why were the following transfers allowed to go through without any warnings?"[14]

During the second hearing of 16 September 2025, the Arbiter admitted this additional evidence to the proceedings and gave opportunity to Service Provider to cross-examine Complainant on this additional evidence.

As there was lack of clarity on the part of the Complainant on the date of the stopped transfer, the Arbiter invited Julian Yeung to explain on behalf of the Service Provider.

Mr Yeung stated:

"***Asked by the Arbiter whether our records show that there was any transaction which was requested by the complainant and we cancelled it, I say, yes, there are instances where there are cancelled transactions. In respect of one of the***

[13] P. 56 - 57
[14] P. 59

wallet addresses, there was scam activity that was detected, but that wallet never received a withdrawal from the complainant.

In respect of the other cancellations, there was a large transaction which was first attempted to be executed which was subsequently carried out after she instructed that we carry out the transaction in a much smaller amount.

The important fact is, in respect of the cancelled transactions, there were only two scenarios.

Where an address has been detected as being involved in scam activity, those transactions are cancelled completely such that no withdrawals to those addresses can be made.

I am asked why Crypto.com stopped a transaction and not others.

The Arbiter understands that one was stopped because the wallet address was signalled to Crypto.com as subject to some fraudulent activity and that transfer was cancelled.

I say that this is correct."[15]

When asked to explain why there were transactions to one of the wallets which were used to transfer the BTC, wallet with code starting 3CJRAR that were also cancelled before the actual transfers took place, Julian Yeung explained:

"Just to be clear, and it's not for me to make their case for them, in their email to the OAFS, there was an attachment which refers to a successfully whitelisted wallet. This is the attachment to the email which the OAFS would have received on the 19th of June, which highlights an address which starts 3EJHP. (Document 63)

If you were to look at the submissions of the service provider presented to the Arbiter at the first instance, you can see towards the end of the submissions, on page 4 of the service provider's reply, that we highlighted the two addresses where the withdrawals were made to.

These start, respectively, with the letters and numbers 3ASJY and 3CJRA.

So, that's to say that the addresses where a successful withdrawal was carried out to was only to these two addresses, whereas the one [the Complainant]

[15] P. 69 – 70

complains of is to a completely different wallet address where no transactions were completed.

So, to make it clear, in respect of the two wallets that we highlight, no scam activity was indicated to us at the time the withdrawals were made.

… …

The first is the whitelisting, the second one is the pending, and the third one is cancelled.

And this is a fraud; a wallet to which no transfers were made.

In respect of the wallet address 3EJHP, no successful withdrawals were made."[16]

During his evidence, Mr Yeung submitted:

"The case at hand concerns withdrawals that were made were made between the 18th of September 2024 and the 26th of September 2024.

The withdrawals were made to two addresses, which are outlined in the service provider's submissions.

Our evidence is that at the time that these transactions were made, there were no indications that they were related to scam activity.

And from the complainant's own evidence, these transactions were carried out by herself, having logged on to the Crypto.com app on her phone.

We would also highlight that at the multiple stages where the withdrawal addresses are concerned, Crypto.com makes many warnings to its users regarding the prevalence of scam activity.

The warnings are given at the time when a new address is added to the whitelisted portion of the withdrawal addresses.

in this section, users are reminded that they should not be withdrawing to addresses that they do not trust. And references are made to an article on Crypto.com warning about the common scam situations which users of cryptocurrency have seen in the past.

The first warning is given when a user adds a new withdrawal address to their account. At this point, users are reminded to only withdraw to addresses that

[16] P. 71

they trust. And, in addition, there is a reference made to articles on Crypto.com warning its users of the common scam activities.

A second warning is given at the time of each and every withdrawal. And, at this point, users are reminded again not to withdraw to users or addresses that they do not trust.

The same reference to an article is made again warning of scam activity. And, in addition, users are reminded not to fall for situations where high returns or unrealistic returns are promised to them.

In addition, we confirm that from our side of the monitoring process, these two addresses, which the user withdrew funds to are non-custodial addresses which are not operated by Crypto.com.

As far as we can tell, these withdrawal addresses are non-custodial accounts; they are not operated by a centralized exchange.

So, on the balance of the foregoing, we would highlight that the user in question, the complainant, authorised the transactions herself.

She was warned sufficiently and numerously at many points of the process that she is to withdraw only to addresses that she trusts and to not fall for the common scam situations. Notwithstanding this, the complainant has chosen to continue with her withdrawals.

And we should not be held at fault for executing transactions which she has given us authority to do so.

As a result of this, we would say that the unfortunate burden of the case is for the complainant to burden herself and that Crypto.com should not be penalized for her unfortunate events.

And as a last submission, all the transactions are carried out in an immutable basis, meaning that they cannot be reversed.

From the evidence at hand, Crypto.com was not made aware of [Complainant's] complaints of having fallen to scam activity until after the last of the transactions had occurred."[17]

[17] P. 68 - 69

Final Submissions

In her final submissions, Complainant stated:

"Crypto.com argues that the subsequent transactions were successful because they were directed to other wallet addresses that were not flagged as fraudulent by the system. However, for an ordinary user, cryptocurrency addresses appear as a random sequence of characters. I could not distinguish one address from another, let alone assess their reliability. These transfers were also executed under the pressure of fraudsters, not on my own initiative and, therefore, there was no genuine 'trust' on my part toward these addresses."[18]

In their final submissions, Service Provider made an evident attempt to walk back on the evidence they had provided during the hearing (as above quoted) that the stopped payment to wallet number starting 3EJhp was due to suspicion of scam involvement related to this wallet and instead stated:

"*The Complainant has referred to a failed transaction involving the attempted withdrawal of 0.223601 BTC to the external wallet address 3EJhp … ('Failed Transaction')*

A multitude of reasons can cause transactions to be blocked. For instance, this may include situations such as, but not limited to, the user's profile, their activity, the size of the withdrawal, or even an erroneous transfer.

While it was stated during the oral testimony of Mr Julian Yeung, that there was a possibility that the Failed Transaction had been blocked due to fraud related reasons, we would highlight that as of the date of this Final Note, there have been no confirmed or flagged warnings received from our third-party vendors or any internal flags indicating the wallet address 3EJhp … is linked to any scams."[19]

Analysis and considerations

Having heard the parties and seen all the documents and submissions made,

Further Considers:

[18] P. 75
[19] P. 81

The Merits of the Case

The Arbiter is considering the complaint and all pleas raised by the Service Provider relating to the merits of the case together to avoid repetition and to expedite the decision as he is obliged to do in terms of Chapter 555[20] which stipulates that he should deal with complaints in '*an economical and expeditious manner'.*

The Service Provider

Foris DAX was at the time of these events licensed by the Malta Financial Services Authority ('MFSA') as a VFA Service Provider as per the MFSA's Financial Services Register.[21] At the time of the transfers subject of this complaint they had a Class 3 VFAA licence granted, on 16 April 2021, by the MFSA pursuant to Article 15 of the Virtual Financial Assets Act, 2018 ('VFAA').

As per the unofficial extract of its licence posted on the MFSA's website, the Class 3 VFAA Licence authorises Foris to provide the following VFA Services: (i) Execution of orders on behalf of other persons (ii) Dealing on own account and (iii) Custodian or Nominee Services to Experienced and Non-Experienced investors.[22]

As outlined in the disclaimer section of the *Crypto.com* website, Foris is *'trading under the name 'Crypto.com' via the Crypto.com app'*. [23]

Observations & Conclusion

Summary of main aspects

The Complainant made the transfers of her digital assets subject of this Complaint using the *Crypto.com* app. The said transfers were made to external wallet addresses thinking the wallet belonged to her as her investment account with *Entrust Capital* which later she discovered were scammers.

[20] Art. 19(3)(d)
[21] https://www.mfsa.mt/financial-services-register/
[22] https://www.mfsa.mt/financial-services-register/
[23] https://crypto.com/eea/about

The transfers to the external wallets were made on the specific instructions of the Complainant.

External wallets are recognised only by their number and their proprietors or beneficial owners are not known to the transferor. The Service Provider had no obligation under the regulatory regime applicable at the time of the transfers to keep or make available information relating to external wallets.

The Complainant *inter alia* claimed that the services provided by Foris were not correct given that it transferred the assets but failed to protect her from fraud and allowed their infrastructure to be used for fraudulent purposes.

She argued the fact that Foris had stopped an initial transaction because they had indications that the recipient wallet was associated with fraud, should have induced Foris to suspect fraud also in the transactions they subsequently allowed, even if the recipient wallets were different and at the time not identified as associated with fraud.

On its part, the Service Provider is, in essence, claiming that it has no responsibility for the payment done by the Complainant as she herself had to verify the transaction information (as per the provisions of the *Crypto.com App Terms of Use*) and that it was not possible for Foris DAX to revoke or reverse the crypto withdrawal once the transaction was done on the blockchain.

They deny that they had any warnings about the fraudulent nature of the external wallets where Complainant transferred her BTC. They also deny that the blockage of payments to one of the recipient wallets had anything to do with suspicion of fraud and was purely for technical reasons.

Applicable Regulatory Framework

As outlined above, Foris DAX was at the time 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 is 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'*[24] 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').

The FIAU[25] also issued Implementing Procedures on the Application of Anti-Money Laundering and Countering the Funding of Terrorism Obligations to the Virtual Financial Assets Sector.[26] Section 2.3 of these Implementing Procedures detail the monitoring and transaction records obligations of VFA licensed entities.

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 her having authenticated the transactions personally, although obviously she was acting under the influence of the scammers.

The Arbiter 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 her account held with Foris to allegedly fraudulent external wallets causing a loss to the Complainant of approximately €32,000.

  The Complainant expected the Service Provider to prevent or stop her transactions. She claimed that the Service Provider had an obligation to warn her of potential fraud especially after they had blocked a transfer that

[24] Guidance 1.1.2, Title 1, *'Scope and Application' of the 'Guidance on Technology Arrangements, ICT and Security Risk Management, and Outsourcing Arrangements'*.
[25] Malta's Financial Intelligence Analysis Unit being the competent authority of AML issues.
[26] Layout 1 copy (fiaumalta.org)

she attempted to make to a wallet which was signalled as potentially fraudulent.

- The Service Provider maintains that the recipient wallets were not under any suspicion of fraud and that the Complainant had declared that she was the owner of or had control over the recipient wallet.

- Complainant must have herself 'whitelisted' the wallet address giving an all-clear signal for the transfer to be executed**.**

  In the process of such whitelisting, as well as in the process of the actual transfers, the Complainant was warned by the Service Provider to ensure that she was responsible for the trustworthiness of the transferee wallet.[27]

  In fact, the Complainant herself did not raise any suspicion or evidence that there was any link between the Service Provider and the external wallet addresses she transferred her BTC to.

- 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 December 2024,[28] several weeks after the last of the disputed transactions was already executed and finalised.[29]

[27] P. 68
[28] P. 11
[29] Crypto transactions may be processed and completed within a few minutes or hours (as indicated on various websites following a general search on the internet).

> Once finalised, the crypto transfer 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).[30]
>
> 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.
>
> 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 …'*.[31]

The Arbiter also 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'*.[32]

These are *'sector-specific Implementing Procedures [which] complement the Implementing Procedures – Part I [issued by FIAU] and are to be read in conjunction therewith'*.[33] 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

[30] E.G. https://www.chargebackgurus.com/blog/chargebacks-more-volatile-complex-than-cryptocurrency
[31] P. 46
[32] https://fiaumalta.org/app/uploads/2020/09/20200918_IPsII_VFAs.pdf
[33] 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[34] and Travel Rule[35] 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. 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 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.*

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

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

VASPs have been long encouraged by the Office of the Arbiter (in decisions dating back from 2022),[36] 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 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.[37]

***Compliance with such recommendations or lack thereof will be taken into consideration in future complaint adjudications**.'*[38]

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**."*[39]

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,*

[36] Such as Case ASF 158/2021
[37] Such as Case ASF 069/2024
[38] Emphasis added by the Arbiter
[39] Emphasis added by the Arbiter

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****; …'.*[40]

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 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

[40] Emphasis added by the Arbiter

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.

General Observations

The Arbiter sympathises with the Complainant for the ordeal she suffered as a victim of a scam.

However, since trading and investing in crypto assets is a new area in the financial services sector, the Arbiter would like to make a few observations.

Apart from the high risks and speculative nature commonly associated in trading with crypto, a consumer venturing in this area needs to be conscious and aware of the additional risks being taken, also, due to other factors including the risks associated with the infancy of the regulatory regime applicable, if at all, to this sector in general which may not provide the same safeguards and protection normally expected and associated with other well-regulated sectors of the financial services sector.

Moreover, given the increasing and alarming volume of scams and fraud existing in the crypto field, retail consumers need to, more than ever, be vigilant and take appropriate and increased measures to safeguard themselves as much as possible to minimise and avoid the risk of falling victim for scams and fraud.

Retail unsophisticated investors would do well if, before parting with their money, they bear in mind the maxim that if an offer is too good to be true, then, in all probability, it is not true.

The Arbiter cannot help but notice the lack of or inadequate knowledge that many retail consumers have with respect to the various risks applicable to this area and on how to better protect themselves, despite the rush by many to join and participate into this sector.

The Arbiter considers that much more needs to be done on this front, apart from in other areas, to better protect consumers. Service providers operating in this field need to also do their part and actively work to improve their onboarding process by evaluating the much-needed knowledge of benefits and risks for consumers who opt to venture into this field.

Decision

As explained above, at the time of the transactions in questions, there was no obligation for the Service Provider to make sure that the recipient wallets belonged to or were under the control of the Complainant.

These obligations entered into force in 2025 through the MiCA and the Travel Rule referred to above.

As the relationship between the parties was very short, and the transactions occurred in a matter of a few days, there was no history which could have triggered signals of something abnormal in the transactions concerned.

Furthermore, the Complainant does not challenge that she had authorised the transfers and must have ignored clear warnings to ensure that she has full confidence in the ownership of transferee wallets.

The only issue which does raise some reason to find the Service Provider partially or fully responsible for the losses suffered by Complainant relates to the fact that the Complainant had been stopped from executing a transfer to a suspicious wallet before[41] she was allowed to make transfers to other recipient wallets which at the time had no signals of potentially fraudulent activities.

The Arbiter is not convinced by the retraction made by the Service Provider in their final submissions that the reason for such stoppage could have been related to issues different from suspicion of involvement of the wallet in fraudulent activities. The contradictory statements were only raised in the final submissions and hence are not acceptable.

The Arbiter bases his judgement on the evidence given under oath by the representative of the Service Provider who categorically admitted that the stoppage of the payment was related to suspicion of fraud.[42]

[41] In her email of 19 June 2025, the Complainant noted that *'… one of the transactions was unexpectedly cancelled, while all subsequent ones were processed without issue.'* (Pg. 59). This was not contested by the Service Provider.

[42] P. 69 - 70 quoted earlier in this decision

The Arbiter has to decide whether the fact that a relatively new customer had her payment stopped because of potential fraudulent issues, should have given rise to additional obligations under the *Duty of Care and Fiduciary Obligations per Article 27 of the VFA Act*.

The Arbiter is of the opinion that the fact that Complainant had a payment stopped for possible involvement of fraudulent transactions should have given rise to concerns, under the Care and Fiduciary Duties, leading to having a good discussion with the client before authorising transfers to what, at the time, seemed 'normal' wallets, almost immediately after the first attempt was blocked.

It would appear logical to suspect that a client who at her first attempt was blocked because she seemed to be dealing with fraudulent wallets, was also dealing with fraudulent activities at her subsequent attempts even if at the time the new recipient wallets were not signalled as suspicious.

Foris must surely be aware of how quick fraudsters move from wallet to wallet the moment an existing one gets suspected of fraud. Some sort of temporary veto on payments until the position is clarified would have been a logical precaution.

On the other hand, the Arbiter does not feel that Complainant should be exempted of all responsibility for her loss given that she exercised a clear dose of gross negligence inspired by greed for illusionary quick and easy profits promised by professional scammers. Full exemption would lead to an undesirable situation of moral hazard where consumers take undue risks through gross negligence expecting high returns without exposure to potential losses.

For the reasons amply stated in this decision, the Arbiter considers the Complaint to be fair, equitable and reasonable in the particular circumstances and substantive merits of the case,[43] and is partially accepting it in so far as it is compatible with this decision.

Given the identified shortcomings outlined earlier, the Arbiter concludes that it is fair, equitable and reasonable in the particular circumstances and substantive merits of the case to award the Complainant the amount of EUR 16,000 (sixteen

[43] Cap. 555, Article 19(3)(b)

thousand euro) being 50% of the loss, with the Complainant bearing the remaining 50%.

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

Alfred Mifsud
Arbiter for Financial Services

Information Note related to the Arbiter's decision

Right of Appeal

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

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

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