Before the Arbiter for Financial Services

Case ASF 228/2024

QP

(the 'Complainant')

vs

OpenPayd Financial Services Malta Limited

Reg. No. C 75580

('OpenPayd' or 'Service Provider [SP] – 1')

vs

Foris MT Limited

Reg. No. C 90348

('FMT' or 'Service Provider [SP] – 2')

vs

Foris DAX MT Limited

Reg No. C 88392

('FDAX' or 'Service Provider [SP] – 3')

Sitting of 18 August 2025

The Arbiter,

Having considered in its entirety, the Complaint filed on 06 December 2024, including the attachments filed by the Complainant,[1]

[1] Page (P.) 1 - 6 and attachments p. 7 - 73

The Complaint

Where, in summary, the Complainant says he is a victim of a scam orchestrated by unknown persons operating through a platform known originally as 'Entricapital' then as 'lloy-dsb' when they claimed to have become part of Lloyds Bank of UK, who persuaded the Complainant to start investing funds promising strong returns.

The first investment was affected on 05 July 2024[2] for an amount of €799 paid through his credit card linked to his account with UniCredit Bank in Rome.[3]

This small investment was reported by the fraudsters to have grown to €13,15.04[4] and this convinced Complainant to transfer larger amount as follows:

REF	DATE	AMOUNT IN €	BENEFICIARY	TRANSFER AGENT
1[5]	22.07.2024	5,000	TrendMark	Modulr Fin. Spain
2[6]	23.07.2024	14,400	TrendMark	Moduilr Fin. Spain
3[7]	01.08.2024	20,000	Complainant	OpenPayd Malta
4[8]	02.09.2024	3,500	Complainant	OpenPayd Malta
5[9]	03.09.2024	5,000	Complainant	OpenPayd Malta
6[10]	18.09.2024	50,000	CR8ATIV GEN.	EASYPAYMENT Spain
7[11]	19.09.2024	15,100	Complainant	EASYPAYMENT Spain

[2] P. 49
[3] P. 38
[4] P. 39
[5] P. 51
[6] P. 52
[7] P. 53
[8] P. 54
[9] P. 55
[10] P. 56
[11] P. 57

REF	DATE	AMOUNT IN €	BENEFICIARY	TRANSFER AGENT
8[12]	30.09.2024	6,000	TrendMark	EASYPAYMENT Spain
9[13]	03.10.2024	15,000	TrendMark	??
10[14]	14.10. 2024	14,990	TrendMark	??
Total		**148,990**		

All payments were made by bank transfers from Complainant's account with UniCredit Rome (payments 1 to 8) and Crédit Agricole Italia – Rome (payments 9 & 10).

In his Complaint there is mentioned an overall loss €163,910 which is €14,920 more than the above-listed payments. It probably includes the €799 initially paid by card and an amount of circa €14,000 which is undocumented. The undocumented amount may include two additional transfers of €7,500 and €5,000 which Foris MT claim to have received from Complainant through OpenPayd also on 03 September 2024.[15]

Complainant adds that his loss has to be topped up with €18,000 interest incurred[16] so he explains the total damage incurred amounts to €181,910. He states that on 22 October 2024, fraudsters were asking for more fund transfers promising that they will transfer back an amount of €301,862.38 and sent him false evidence (QONTO), showing funds were ready for transfer thus realising huge profits on his investments.[17]

Obviously, these funds were never received.

[12] P. 58
[13] P. 59
[14] P. 60
[15] P. 372 - 373
[16] P. 39
[17] P. 23

In his Complaint to the OAFS, payments above listed with reference 1, 2, 6 - 10 are irrelevant as the intermediary is not a licensed institution that can be considered as a Service Provider in terms of CAP 555 of the Laws of Malta.

The Complainant against OpenPayd relates to payment 3 - 5 amounting to €28,500.

His claim against FMT and FDAX is for €41,000 being the above-mentioned €28,500 which OpenPayd passed on to Complainant's account with FMT and two payments for €12,500 received in the Complainant's account with FMT from other channels or from OpenPayd but not specifically listed in the Complaint.[18]

For proper understanding of the Complaint, it is clarified that FMT received funds totalling €41,000 as above explained and, with instructions from Complainant, these were then converted in crypto assets which were then transferred to Complainant's digital wallet with FDAX who then transferred them as instructed by Complainant (under the guidance of the fraudsters) to external wallets controlled by the fraudsters.

However, in total, Complainant is requesting a total compensation of €71,100 from the three Service Providers included in his Complaint being the actual funds transferred of €41,000, an element of interest he lost or incurred, and some allocation of other expenses (including interest on borrowed funds) under an unclear formula he devised that takes into account all the payments that were made to fraudsters and not only those related specifically in this Complaint to the OAFS.

The Complainant admits that in the process of the execution of this fraud, he gave the scammers access to his secret credentials by onloading the application 'AnyDesk' and 'AnyViewer' which basically gives an authorised third party full access to his banking and investment accounts as if he was doing them personally.[19]

Important observation

While the Complaint has been explained above in a single process, the replies of the respective Service Providers, the hearings and evidence collection process,

[18] See footnote 15
[19] P. 41

the Arbiter's analysis, observations and, ultimately, final adjudication decision will be separate for each Service Provider as they operate under licences with different obligations and regulations and cannot be held responsible except for their own claimed participation in this fraud journey.

Foris MT Limited

The Complaint against FMT is the simplest to deal with, and the Arbiter is accordingly addressing it first to reduce the complexity of this case.[20]

During the procedure it was not contested that:

- Complainant opened an account with FMT (with the assistance and under guidance of the fraudsters).
- FMT received €41,000 in funds in the Complainant's account showing Complainant as the remitter.
- Complainant gave instruction for these funds to be exchanged in digital assets (more details on this is the case against FDAX) and to transfer these digital assets to the Complainant's wallet with FDAX.
- At no time was FMT involved in any change of beneficiary of the funds either in fiat currency (€41,000) or in digital assets (USDT 21,224.95 and BTC 0.3860232).[21]
- The funds were received in FMT Euro account with OpenPayd and were transferred as digital assets to Complainant's account with FDAX.
- FMT was not involved in the transfer of digital assets to an external wallet controlled by the fraudsters.

Given these uncontested facts, the Arbiter sees no reason why FMT – [SP]-2 should be held responsible for the losses sustained by the Complainant when the fraudsters gained control of his funds/assets.

[20] Reply from Foris MT Ltd was received 4 days after the 20 days statutory period. Reasons were explained in their e-mail of 10.01.2025 (p. 139). In accordance with established policy, Arbiter waived contumacy rules to allow fair hearing during arbitration proceedings which the law stipulates should be conducted with informality.
[21] P. 143 erroneously show 0.1313928 BTC but Fig. 4, p. 147 and Fig. 8, p. 149 show above indicated BTC acquisitions.

In view of the above, the Arbiter is dismissing the Complaint against Foris MT Limited. However, in view of the complexity of the Complaint, they are ordered to bear their own costs of these proceedings.

Foris DAX MT Limited

In their reply[22] of 03 January 2025, FDAX stated:

> '*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 "**Fiat 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. EUR fiat deposits and withdrawals are facilitated through our banking partner, OpenPayd Financial Services.*
> - *Mr … (the "Complainant"), e-mail address … … … ... became a customer of Foris DAX MT Limited through the Crypto.com App and was approved to use the Wallet on 18 July, 2024.*
> - *The Company notes that in the submitted complaints file, (the Complainant) has outlined the desired remedy as: (i) reimbursement for incurred financial losses.'*[23]

They then gave a detailed timeline how the €41,000 referred to under the case of FMT were received in the Complainant's wallet in digital assets as follows:

[22] P. 85 - 97 with attachments p. 98 - 124
[23] P. 85

Date	Amount in Euro	Digital assets by conversion of Euro net of charges
05.08.2024	20,000	USDT 21224.95
02.09.2024	3,500	BTC 0.0656964
03.09.2024	7,500	BTC 0.3203268
03.09.2024	5,000	
03.09.2024	5,000	
Total	**41,000**	

The timeline also includes details how some digital assets were exchanged into other digital assets, and how between 5 August2024 and 4 September 2024, USDT 26,068.99 and BTC 0.2854488 were transferred to four different external wallets (apparently controlled by the fraudsters) through 34 different transfers.

They 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 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 an 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.[24]

Hearings

During the hearing of 22 April 2025, when Complainant was asked to explain why he is expecting compensation much bigger than the amount of the funds transferred, he explained:

'(The Complainant) has explained that overall, from the three service providers involved in this complaint, he is expecting €71,000 which is the actual money he has transferred plus the consequential losses by way of lost interest and other gains which he is seeking. So, on top of that, he is topping up the €41,000 to €71,000 as he has explained to us (pro rata).'[25]

On being cross-examined, he stated:

'Asked whether it is correct to state that I knowingly and with my consent granted permission to my financial advisors to give them control of my mobile phone and my Crypto.com App an account and that I gave them access to control everything, I say, yes, I confirm.'[26]

[24] P. 95 - 97
[25] P. 501
[26] *Ibid*.

During the evidence of the Service Provider, during the hearing of 09 June 2025, it was stated:

'The complainant became a customer of Foris DAX MT through the Crypto.com App on 18 July 2024, and the starting point of the transactions involving Foris DAX MT began on Monday, 5 August, with the purchase of the cryptocurrency USDT using approximately €20,000. Through a series of transactions from 5 August to 4 September, (the Complainant) withdrew cryptocurrencies primarily to four external addresses: two involving USDT and two involving BTC, which is also known as Bitcoin.

In handling these transactions, we can only see that Foris DAX MT has carried out the instructions of (the Complainant) or those who were controlling his account. We say that because we understand that, at some point, (the Complainant) gave control of his account through an AnyDesk App function which allows third parties to control the device which link is drawn to between the two mobile devices such that (the Complainant) himself gave third parties access to his account whether directly through this AnyDesk procedure through the use of his own unique login credentials, or he carried out the instructions or transactions pursuant to instructions given to him by third parties.

We say that at each point before the four wallet addresses in question were able to be added to the Crypto.com App account for withdrawals. There have been adequate warnings given to (the Complainant) as to who and what persons he should be whitelisting on his account. The whitelist function enables you to withdraw crypto assets to third-party wallets.

None of these four cryptocurrency wallets were controlled or operated by Crypto.com, and (the Complainant) was given the warning that he should only be making cryptocurrency transfers to people he trusts. He should not be making cryptocurrency transfers on platforms or to people who promised high returns or suspiciously high returns. He was warned as to the presence of scams in the cryptocurrency sphere by reference to an article on the Crypto.com website and, all in all, these warnings will have presented themselves not only at the time the withdrawal addresses were added, but also before each and every transaction that (the Complainant) carried out. These warnings exist because, as we've warned in the warning itself,

cryptocurrency transactions are instant, they are immutable and cannot be reversed.

On our side, we will say that (the Complainant), unfortunately, has led himself to being scammed by third parties as since he did not pay heed to our warnings, he did not take out the necessary steps to carefully ensure that he himself was the one who was transacting on his account. And more importantly, we can see that at all times he had relied on third parties and their instructions to carry out the cryptocurrency purchases and withdrawals that he made.

Foris DAX MT can only carry out instructions pursuant to the user's instructions and we have carried out those transactions and withdrawals faithfully, accurately and as instructed by (the Complainant) himself to the extent that the transactions were not performed by (the Complainant) himself. He was the one who gave access to the account to third parties, and he himself was grossly negligent in protecting the security of his account.

So, all in all, we would say that there is no case against Foris DAX MT. We have only carried out the transactions according to his instructions. We have provided adequate warnings on multiple occasions at the start of the cryptocurrency journey when he added these withdrawal addresses as well as at each time these withdrawals were made to the separate accounts on the separate occasions. Crypto.com does not operate the four wallets in question and does not have any information as to who operates these accounts, or the comings and goings of cryptocurrency. And, in any case, cryptocurrency transactions cannot be reversed as at the point of instruction, they become immutable and irreversible.'[27]

...

'I can confirm that at the time the transactions were made, there were no warnings on our own internal systems as well as those provided by third parties who we employ for the purposes of transaction monitoring. There were

[27] P. 503 - 505

no indications that these addresses were linked to fraudulent behaviour or scam activity.'[28]

Complainant did not cross-examine the evidence of FDAX.

Analysis and Observations

Having heard the parties

Having seen all the documents

Considers

Applicable Regulatory Framework

FDAX 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, FDAX 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'*[29] 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').

[28] P. 505

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

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, even though he argues he was being guided by the fraudsters to whom he willingly and with gross negligence disclosed his secret access credentials.

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 FDAX, to unknown external wallets.

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

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

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

The transfer was rather indicated to have been done to an *'external wallet'* and hence the Service Provider had no information about the third party to whom the Complainant was transferring his crypto assets.

- The Complainant seems to have only contacted the Service Provider on 01 November 2024[30] some 2 months after the last of the disputed transactions was already executed and finalised.[31]

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).[32]

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 FDAX.

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 …'.[33]

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.

[30] P. 29
[31] 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).
[32] E.G. https://www.chargebackgurus.com/blog/chargebacks-more-volatile-complex-than-cryptocurrency
[33] P. 96

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'*.[34]

These are *'sector-specific Implementing Procedures [which] complement the Implementing Procedures – Part I [issued by FIAU] and are to be read in conjunction therewith'*.[35] Section 2.3 of these Implementing Procedures detail the monitoring and transaction records obligations of VFA licensed entities.

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

Failures of the Service Provider in respect of AML/CFT are not in the remit of the OAFS and should be addressed to the FIAU. In the course of these procedures, no such failure was indeed alleged.

The Arbiter shall accordingly not consider compliance or otherwise with AML/CFT obligations in this case.

ii. MiCA and the Travel Rule

As to the identification of the recipient of the funds, it is noted that MiCA[36] and Travel Rule[37] obligations which entered into force in 2025, and which give more

[34] https://fiaumalta.org/app/uploads/2020/09/20200918_IPsII_VFAs.pdf
[35] 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'*
[36] EU Directive 2023/1114 on markets in crypto assets https://eur-lex.europa.eu/legal-content/EN/AUTO/?uri=celex:32023R1114
[37] 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

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. 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[38] 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),[39] 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

[38] *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

[39] Such as Case ASF 158/2021

accounts of retail customers and disappear such funds in the complex web of blockchain anonymous transactions.[40]

Compliance with such recommendations or lack thereof will be taken into consideration in future complaint adjudications.'[41]

The Arbiter will, however, 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.'[42]

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****; …'*.[43]

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

[40] Such as Case ASF 069/2024
[41] Emphasis added by the Arbiter
[42] Emphasis added by the Arbiter
[43] Emphasis added by the Arbiter

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 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 some two months when the fraudulent transfers were happening in relatively consistent quantity values in funds transferred from Complainant's account with banks in Italy.

Furthermore, there is no issue regarding the obligations to safeguard and protect Complainant's assets as these were only transferred out to third parties on the verified instructions of the Complainant.

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

Decision

There should be no doubt that 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.[44]

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.

It is quite possible for Complainant to consider whether there is a case to explore enquiries with his Italian banks which under the PSD 2,[45] have a much more

[44] 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/

[45] EUR Directive 2015/2366 – Payments Services Directive

relevant obligation for effective transaction monitoring systems to protect their client with whom they have had a long-term relationship with deep KYC information.

There may be a case for arguing that with their knowledge of the Complainant, the banks could have alerted the Complainant to the possibility of fraud, especially as many payments were involved beyond what was handled by local Service Providers in this Complaint. No evidence was forthcoming that Complainant has lodged such formal complaint with his Italian banks other than requested recalls which were unsuccessful.

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.[46]

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.

OpenPayd Financial Services Malta Ltd

The case against OpenPayd is different from the complaint against FMT and FDAX as Complainant maintains that he had no account with OpenPayd and, therefore, they should have returned the 3 transfers for a combined value of €28,500 to the remitter, being himself, through his Italian Bank UniCredit.

He specifically states:

[46] 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

'***OpenPayd Financial Services Malta Ltd has accepted three bank transfers from me to me even though I do not have an account with them nor have I explicitly authorized anyone to operate on a non-existent account.***

When I contacted OpenPayd, they closed the case, rejecting all responsibility and all my requests. My arguments are:

1. ***Transfers are made in my name on my behalf but I have never been the holder of account, nor have I ever authorized withdrawals from third parties unknown to me on the non-existent account. To my banking knowledge no one can operate without having a current account, nor can operate on a given account without an express written delegation from the account holder;***

2. ***They are part of the fake trading scam demonstrating and discussed in the attached application form, for this reason I believe that they must be refunded to me since the corresponding operations are not transparent nor regular.***

For the sake of completeness, I would like to point out that I filed a complaint with the local police (Carabinieri) in Rome, Via Mentana 15, in November 2024.'[47]

Although, in his Complaint, Complainant only made reference to three payments totalling €28,500 which were sent to OpenPayd,[48] from the proceedings against FMT above referred to, there were two further payments amounting to €12,500[49] which were also sent through OpenPayd on 03 September 2024 bringing the total funds transferred through OpenPayd and then sent to FMT to €41,000.

In their reply of 06 January 2025, OpenPayd raised a preliminary plea challenging the Arbiter's competence to hear the case against them as they maintained that Complainant was not their 'eligible customer' as defined in Article 2 of CAP 555 of the Laws of Malta and, consequently, in terms of Article 11(1)(a) and Article 19(1) of the same Act CAP 555, the Arbiter cannot adjudge this Complaint.

[47] P. 3
[48] p. 17 - 19
[49] P. 372 - 373

After hearing both sides' arguments about this preliminary plea at a hearing held on 22 April 2025,[50] the Arbiter issued a Decree on 02 May 2025[51] dismissing the preliminary plea as he considered Complaint as an eligible customer once the transfers were clearly showing himself as beneficiary of the transfers, and this is considered as having requested a service from the Service Provider as provided in the definition of eligible customer.

The Arbiter made reference to a similar decision he issued in case ASF 155/2024 involving the same Service Provider.[52]

The first hearing on the merits was held on 14 May 2025, where the Complainant stated:

'The Arbiter has summarised that in a perfect way. I apologise if I will repeat something during my exposition.

OpenPayd Financial Services, in addition to the claim that I have never been its client, a claim which has been decreed not true by the Arbiter, has advanced other claims which I want explicitly to challenge here.

I will start by considering that, in normal circumstances, a sum reported on bank transfers sent to a financial operator is credited to the beneficiary in a current account, and I, as the beneficiary of all the three payment orders already known, I should have had a current account contract with OpenPayd. If that account does not exist, as OpenPayd claims with the statement "OpenPayd has no contractual relationship with you", according to good financial payments practices, the financial operator should have rejected the transfer to the sender, with the reason "unknown recipient".

This was not done by OpenPayd, nor, as recipient of the transfers, I received money in any form of payment, and even only for this, at least as the sender, I claim to have suffered a "compensable" damage due to the negligent conduct which I explicitly charge to OpenPayd in its professional role of financial operator.

[50] P. 152 - 155
[51] P. 156 - 158
[52] https://financialarbiter.org.mt/sites/default/files/oafs/decisions/2097/ASF%20155-2024%20-%20PU%20vs%20OpenPayd%20Financial%20Services%20Limited.pdf

Moreover, at date 2024/12/18, my bank Unicredit Agency 3660 in "Sapienza" University of Rome, on my request, directed to OpenPayd three official recall with the reason "scam", totalling the entire transferred sum of Euros 28,500.

To these requests of recall, OpenPayd didn't even bother to answer and this negligent conduct is contrary to the obligations of collaboration between financial operators provided by the European PSD2 legislation.

I want to explicitly challenge also another plea by OpenPayd. In the same email at 2024.11.2, previously referred to, it stated:

"All services that have been provided to you, including the opening and management of your account, have been performed directly by Foris MT Limited" and "The payments were made and processed by you and authorised through its issuing banks in favour of Crypto.com."

I never, in any form, issued bank transfer payable to Crypto.com nor in favour of Foris MT Limited, contrary to what was asserted by OpenPayd. Indeed, all the considered three bank transfers are payable to me. Moreover, my bank acts only on my behalf. At no point in the current account relationship between me and my bank it is provided that the bank can act on my account on its own behalf. My bank (and I believe no bank in the world) is not provided for the prerogative to independently issue an order in favour of third parties. Nor a third party can replace the account holder to carry out transactions in the absence of written and legally validated delegation. The only way for a bank to transfer money to third parties is by making on the part of account holder a transfer payable to the beneficiary's name. And, as I said, I never, in any form, issued bank transfer payable to Crypto.com.

Moreover, OpenPayd stated:

"All services that have been provided to you, including the opening and management of your account, have been performed directly by Foris MT Limited."

This leads me to ask: which legally recognised methods were used by OpenPayd for transferring to Foris MT Limited money destined to me? In particular, according to which statutory provisions did OpenPayd considered that the sums corresponding to the bank transfers all payable to me, given the

alleged non-existence of an account in my name were in their own availability and, therefore, were considered transferable to Crypto.com, without even informing me."[53]

During cross-examination, Complainant stated that:

a. he does not think that OpenPayd was part of the scam but he has no means to know if the fraudsters, who had indicated to him to send his funds to OpenPayd, were known to OpenPayd or they simply made use of facilities offered by OpenPayd to all customers. He reported as such in the report he filed with the Italian Carabinieri;

b. the IBAN number shown on the transfers to OpenPayd were provided to him by the scammers;

c. he was instructed by the scammers to name himself as the beneficiary;

d. he did not lodge a complaint with UniCredit as he thinks that from their end everything was regular;

e. he lodged complaints against other institutions that handled his payments which are not part of this Complaint;

f. he confirmed that when a UniCredit employee tried to stop the payment of €6,000[54] on 30.09.2024 as their internal systems had flagged 'false trading', he still insisted that the payment be effected. This happened after more than €100,000 had already been transferred and after that, a payment amounting to approximately €14,000 was still made but through Crédit Argricole.[55]

On being pressed by the Arbiter to explain why he put his name as beneficiary of the transfers to OpenPayd when he knew he had no account with them and the funds were intended to reach his account with the fraudsters through his account with Crypto.com, the Complainant stated:

[53] P. 160 - 162
[54] P. 42
[55] P. 166 – Note however that, in fact, 2 payments were made through Crédit Agricole after the payment of €6,000, on 03 October for €15,000 (p. 59) and on 14 October 2024 for €14,990 (p. 60).

'Indeed, I was surprised with this when I read from my documentation when I presented my denouncement to the Carabinieri.

Asked again by the Arbiter why I put my name as beneficiary in the transfer when I knew that I did not have an account with OpenPayd, I say, only because I made the trading operation with my financial advisor who dictated to me to write it this way, thank you and that's all.

I confirm that the advisor/fraudster told me to put my name as beneficiary.

It is being said that I knew that I was naming myself as beneficiary although I knew that I did not have an account with OpenPayd; and I knew that this money wasn't destined to stay at OpenPayd for it was going to make the investments which the fraudster was indicating to me.'[56]

After the hearing, the Complainant provided a copy of his report of the scam to the Carabinieri,[57] evidence of recall made by UniCredit on OpenPayd,[58] and the latter's refusal dated 19 May 2025.[59]

At the last hearing of 09 June 2025,[60] the Service Provider presented their evidence by explaining how the Virtual IBAN (VIBAN) which is declared in the bank transfers related to the account they hold in name of Foris MT Limited and, hence, why the funds were transferred to that account notwithstanding that the beneficiary on the transfers was named as the remitter and not the account holder of the VIBAN.

On being asked why in their reply to UniCredit's recall, they stated that the recall was refused by the beneficiary when the beneficiary on the transfers was himself and he did not refuse them, the Service Provider considered the beneficiary to be the account holder of the VIBAN quoted in the transfers.

[56] P. 167
[57] P. 169 -170
[58] P. 208 - 211
[59] P. 221 - 222
[60] P. 223 - 226

Analysis and Observations

To avoid repetition, the Arbiter refers to proceedings of case ASF 155/2024 which relate to similar circumstances and which the Arbiter had ruled that the Service Provider had no authority to take the provisions of PSD 2 as applicable to normal IBANs and apply them to VIBANs which are not covered by regulation and presented more risks to consumers than normal IBANs. In that case, Arbiter ruled for full refund to the scam victim.

This Complaint, however, presents a very different set of circumstances than those applicable for case ASF 155/2024.

Whereas in that case the Complainant was a vulnerable old person who could not be expected to understand the manoeuvres of the scammers, in this case, the Complainant is an economics professor at an eminent university in Rome who had a clear understanding that the transfers were not destined to his account with OpenPayd but that OpenPayd was a mere transit medium for the funds to reach the investment platform of the scammers who were promising huge returns on his investments.[61]

It is greed that was forcing the Complainant to continue transferring funds to the scammers in spite of growing doubts on their authenticity as evidenced by his declaration in the Complaint:

'The latest masterpieces of the self-styled consultant are the payment of the remaining 71,000 euros of my account on three dates, respectively of 50,000, 15,000 and 6,000 motivated in the manner described shortly. However, it must first be stated that, on 09.19.2024, I received a PDF signed by Claudio Romano and his alleged manager Frank Graham, a communication addressed (so it appears) to the supervisory authorities Bank of England and FCA (Financial Conduct Authority) in which the closure of my "investment account" is reported. The communication records in my favor the sum paid by me of eur 115,100 of which 15,100 as taxation, and a profit (in theory due to me) of eur 124,950.35 from the various operations. The document is inserted here among the documentation. This communication was preceded by two payments of €50,000 (with the justification that it was necessary to lower the

[61] P. 23

profit/investment ratio to fall into the lower tax bracket than the current one) on 18_09, and €15,100 to meet my taxpayer duty in the UK on 19_09. Finally, I was asked to make a final payment, made through Unicredit, of €6,000 which was motivated by the need for "the Lloydbankers administration to unblock" the payments in my favor. The story of the €6,000 payment is worth telling, because, when I made the transfer to the Unicredit branch at La Sapienza University, the employee warned me that the payment had been blocked by the system. The Unicredit branch manager I spoke to explained that the bank to which it was directed had been reported as being engaged in "false trading" by their internal control system. It should be noted that the transfer of 6,000 euros is the smallest of the sums of transfers made by me, and that the bank and the counterparty in question had already been beneficiaries, in the two previous days, of the two payments of 50,000 and 15,000, without any notification being sent to me by Unicredit, and that would have at least alerted me to the possibility of a scam in progress. In their excuse there is the circumstance that both tansfers had me as the beneficiary and only in the reason for payment did the real beneficiary appear with the name CR8ATIV24 -JJ5018. Among others, Unicredit was prompt, after the transfer of €6,000 that I insisted be made anyway (to unblock the alleged payments promised to me), with the signature of a release in favor of Unicredit, to suspend my online account, on several occasions, until my subsequent complaints and requests for reactivation, while no objection had ever been raised to other payments in the months of July and August. From all this whirlwind of accounts and payments, my savings dropped from the initial sum of eur 132,000 on July 8th when the story began, to eur 723.25 on Unicredit at the end of September 2024."[62]

As explained, two further payments were made to scammers from Crédit Agricole (on the presumption that UniCredit refused to make further payments) for some €30,000 in October 2024. This may explain the Complainant's reluctance to lodge a complaint against his Italian Banks and is seeking refuge from intermediaries with whom his relationship was very transient.

[62] P. 42

Decision

As decided in case ASF 155/2024 (which is under appeal), OpenPayd had no authority to credit the funds to the owner of the VIBAN account shown in the transfers instead of the named beneficiary without specific authority from the remitter.

Consequently, the Arbiter feels that this breach of conduct should be reported to MFSA (Malta Financial Services Authority) for proper investigation as the regulator for financial services who licensed the Service Provider. A copy of this decision is being sent to the MFSA.

However, all considered, especially the Complainant's admittance that:

'***I knew that I was naming myself as beneficiary although I knew that I did not have an account at OpenPayd; and I knew that this money wasn't destined to stay at OpenPayd for it was going to make the investments which the fraudster was indicating to me,"***[63]

leaves no doubt in Arbiter's mind that the loss incurred by the Complainant was caused by his gross negligence and not by the conduct failure of OpenPayd. The Arbiter sees no direct causation of the regulatory failure on the part of OpenPayd to the losses suffered by the Complainant. This is reaffirmed by the fact that Complainant continued to make transfers to scammers even after receiving a very clear warning from UniCredit as afore mentioned.

For these reasons, the Arbiter is dismissing this Complaint and orders parties to carry their own costs of these proceedings.

Alfred Mifsud
Arbiter for Financial Services

[63] P. 167

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.