Before the Arbiter for Financial Services

Case ASF 005/2025

LK

(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 31 October 2025

The Arbiter,

Having considered in its entirety, the Complaint filed on 08 January 2025, including the attachments filed by the Complainant,[1]

[1] Page (P.) 1 - 7 and attachments p. 8 - 53

The Complaint

Where, in summary, the Complainant says he is a victim of a scam orchestrated by unknown persons who introduced themselves as Piotr Nikonowicz and Dmitri Bosnia who induced him to make various transfers for investment purposes on a platform titled 'myexpert100.com'.

These transfers were affected from his bank in Latvia, Citadele Banka, to an account which the scammers told him that he has with OpenPayd. He confirmed he had no direct contact with OpenPayd but he knew he had opened a crypto wallet and thought that his account with OpenPayd was connected to his crypto wallet.[2] The wallet was with Crypto.com.[3]

Complainant confirmed that the scammers used to guide him to define himself as the beneficiary of the funds being transferred from his bank even though he knew he never opened an account with OpenPayd and that the funds would finish on his Crypto.com wallet and, eventually, on his 'myexpert100.com' fraudulent platform[4] which at the time did not seem to him as fraudulent.

The transfers effected are listed as follows:

REF	DATE	AMOUNT IN €	BENEFICIARY	Transferree Bank[5]
1[6]	02.12.2024	10000	Complainant	OpenPayd
2[7]	04.12.2024	10100	Complainant	OpenPayd
3[8]	04.12.2024	9900	Complainant	OpenPayd
4[9]	06.12.2024	9900	Complainant	OpenPayd

[2] P. 89
[3] P. 88
[4] *Ibid*.
[5] OpenPayd does not have a banking licence but was indicated as a bank in the payment orders of Citadele Banka
[6] P. 23
[7] P. 13
[8] P. 15
[9] P. 17

REF	DATE	AMOUNT IN €	BENEFICIARY	Transferree Bank[5]
6[10]	06 12 2024	6400	Complainant	OpenPayd
7[11]	06 12 2024	9000	Complainant	OpenPayd
	TOTAL	**55300**		

All payments were made by bank transfers from Complainant's account with Citadele Banka (Latvia).

His complaint was initially filed against SP -1 (OpenPayd) and SP-2 (Foris MT). However, during the hearing against SP-2 of 27 May 2025, the Arbiter decreed that as the transfers of crypto assets to the alleged fraudulent wallets of the scammers were effectively made by a related company, Foris DAX MT, the latter was included as an additional Service Provider SP-3 in the proceedings. [12]

In summary, in his formal complaint, he stated:

"*The main complaint is lack of sufficient safeguards to prevent fraudsters from manipulating official channels and deceiving customers. I was certain that I was using the official platform because the documentation provided appeared authentic. My belief in the platform's legitimacy was further reinforced when I successfully made two withdrawals of funds. This gave me the impression that my investments were being handled properly and securely. Even after the fraudulent redirection my account on the official crypto.com platform remains active, which further blurred the lines between the legitimate and illegitimate entities. It is the responsibility of a financial service provider to ensure that customer accounts, data and the transactions are secure.*

In this case, the provider failed to detect and prevent the unauthorized use of my credentials or to identify the suspicious activity on my account that should've raised the concern. The lack of adequate measures to verify the integrity of the communication channels and transactions allowed fraudsters to convincingly

[10] P. 19
[11] P. 21
[12] P. 303

impersonate the official platform. This undermined my trust in the system and exposed me to financial losses. This redirection to a fraudulent platform www.myexpert100.com through crypto.com underscores a failure in verifying the integrity of external platforms interacting with customer accounts. This negligence facilitated the scam and left me exposed to financial loss."[13]

By way of compensation, he expects full refund of his loss of €55,300 but does not specify from which of the respondents he expects such refund.

The reply from the three respondents will be considered below in separate analysis regarding their role in this complaint.

The Arbiter must first deal with some preliminary issues.

Contumacy

The Arbiter

- Considered that the reply of OpenPayd was filed 3 days later than the 20 days limit contemplated by article 22(3)(c) of the Act Chapter 555 Arbiter for Financial Services.
- 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 complaints 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

[13] P. 4

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

For these reasons, the Arbiter will henceforth apply contumacy 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 will not be applying contumacy rules against OpenPayd.

Competence of the Arbiter

In their reply[14] of 20 February 2025, OpenPayd argued that in terms of Article 11(1)(a) and Article 19(1) of Chapter 555 of the Laws of Malta (Chapter 555 is an Act that defines the operations of the Office of the Arbiter), the Complainant is not an 'eligible customer' as defined in Article 2 of the Act and, therefore, the Arbiter has no competence to hear and adjudicate this complaint.

At the hearing of 27 May 2025,[15] the Arbiter overruled this preliminary plea and proceeded to hear the merits of the case. The Arbiter is hereby explaining his decision for overruling the preliminary pleas.

The transfers complained of show as beneficiary the Complainant without any reference to any third-party beneficiaries. Nowhere in the transfer payment is there any reference to the Merchant/Corporate Client to whose account the Service Provider is claiming to have credited the funds.

[14] P. 76 - 80
[15] P. 87

Article 22(2) of Chapter 555 of the Laws of Malta ('the Act') stipulates that:

"Upon receipt of a complaint, the Arbiter shall determine whether the complaint falls within his competence."

Moreover, in virtue of Article 19(1) of the Act, the Arbiter can only deal with complaints filed by **eligible customers**:

*"It shall be the primary function of the Arbiter to deal with complaints filed by **eligible customers** through the means of mediation in accordance with Article 24 and where necessary, by investigation and adjudication."*

The Act stipulates further that:

"Without prejudice to the functions of the Arbiter under this Act, it shall be the function of the Office:

*(a) To deal with complaints filed by **eligible customer.**"*[16]

Article 2 of the Act defines an *"eligible customer"* as follows:

*"a customer who is a consumer of a financial services provider, or to whom the financial services provider has offered to provide a financial service, or **who has sought the provision of a financial service from a financial services provider**."*[17]

The Arbiter has primarily to decide whether the Complainant is in fact an **eligible customer** in terms of the Act.

No claim has been made that the Complainant was a customer, consumer of the Service Provider or that the Service Provider had offered him any service. The case revolves on whether the Complainant had sought the provision of a financial service from OpenPayd.

On a similar issue in case reference ASF 155/2024,[18] the Arbiter had decreed that as the beneficiary was clearly indicated as being the remitter himself, the Arbiter did not accept that the Complainant:

[16] Article 11(1)(a)
[17] Emphasis added by Arbiter
[18] https://financialarbiter.org.mt/sites/default/files/oafs/decisions/2097/ASF%20155-2024%20-%20PU%20vs%20OpenPayd%20Financial%20Services%20Limited.pdf

"never sought the provision of a financial service from (OpenPayd)."

For same reasons already explained in ASF 155/2024, the Complainant is deemed as qualifying as an *"eligible customer"* in terms of Article 2 of the Act.

Therefore, the Arbiter decrees that he has the competence to deal with the merits of this Complaint, without any prejudice to the complaint against the other co-defendant Service Providers and will proceed accordingly.

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, 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 (FMT – SP 2)

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.

During the proceedings, it was not contested that[19]:

- Complainant opened an account with FMT (with the assistance and under guidance of the fraudsters).
- FMT received €55,300 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 or in digital assets.

[19] P. 300 - 303

- 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 should be held responsible for the losses sustained by the Complainant when the fraudsters gained control of his funds/assets.

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

Foris DAX MT Limited (FDAX – SP 3)

In their reply[20] of 03 January 2025, FDAX stated:

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 Cash (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@gmail.com*, became a customer of Foris DAX MT Limited through the Crypto.com App and was approved to use the Wallet on 28 November 2024.*

[20] P. 505 - 512 with attachments p. 513 - 522

- *The Company notes that in the submitted complaints file, the Complainant has outlined the desired remedy as: (i) reimbursement for incurred financial losses."*[21]

They then gave a detailed timeline how the €55,300 referred to under the case of FMT were received in the Complainant's wallet in digital assets as follows:

Date	Amount in Euro	Digital assets by conversion of Euro
02.12.2024	10000	ETH 2.80879
04.12.2024	10100	ETH 5.45762
04.12.2024	9900	
06.12.2024	9000	ETH 2.70000
06.12.2024	6400	ETH 2.20000
06.12.2024	9900	ETH 1.74001
Total	**55300**	**ETH 14.90642**

The timeline also includes details how ETH 14.85642 digital assets were transferred (after deduction of charges) to an external wallet (apparently controlled by the fraudsters) through 10 different transfers between 02 and 09 December 2024.

They concluded that:

"In summary, it seems conceivable that the Complainant has been the victim of an alleged scam. However, due to the nature of the external wallet and the fact that it is not hosted or operated by the Company, we can neither confirm nor deny this.

[21] P. 505

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

As outlined above in the Foris DAX MT Limited Terms of Use, the Complainant is solely responsible for the security and authenticity of all instructions submitted through the Crypto.com App and, as such, the Company cannot accept liability for the veracity of any third party or for the instructions received from the Complainant themselves."[22]

Hearings

The evidence given in the hearing of 27 May 2025, in the case against FMT, was adopted to apply to this complaint to avoid repetition.

Complainant confirmed that he opened an account with Crypto.com and was provided with a Crypto wallet. He explained that the crypto assets were first transferred to his wallet and then transferred by fraudsters to another wallet which turned out to be fraudulent.[23]

When cross-examined, he stated:

"I say that I have opened an account with Crypto.com but not by myself but with the assistance of the fraudsters. They said that they will help him open an account and also guided him which buttons to push.

Asked how this opening of the account was done, I say that it was over the telephone. They communicated over the telephone and told me what to push.

I say, yes, they saw my telephone screen.

Asked how the fraudsters saw my telephone screen, I say that they sent a link through the application which I opened and then, they connected to my telephone screen with that application.

Asked what is the name of the connection that I used, I say Supremo.

[22] P. 512
[23] P. 300

I am referred to my complaint, where I filed (starting from page 45) what appears to be screenshots of my Crypto.com App account showing the deposits that I made.

Asked whether this is correct, I say, yes that is correct.

Asked to confirm that during the whole process, I had access to my Crypto.com account as well, I say, yes, I too had access to the Crypto.com account.

I confirm that I saw incoming deposits into that account and, also, the outgoing transactions which were assisted by those fraudsters. When I asked them why the amount of the Crypto.com Wallet does not agree; incoming payments are coming into one Wallet and the outgoing payments, another Crypto.com Wallet number appears. They explained that one is used for incoming transactions and another for outgoing transactions.

Yes, it is correct to say that through this entire time the fraudsters were granted access and visibility of my Crypto account by me.

Asked when was it that I realised that I had been defrauded by the scammers, I say that it was around 16 December when I understood that there were two Crypto Wallet account numbers which were being used with the incoming and the outgoing transactions, because the fraudsters indicated which Crypto Wallet account number were to be put in specific transactions.

I say, yes, the fraudsters had given me a Wallet address to make withdrawals to.

It is being said that I followed the instructions of these fraudsters and made the withdrawals myself within my Crypto.com Wallet. I say that this is correct because they told me that they needed that number for the transaction to be made and I understood that I was making transactions to my sub-Wallet. I thought that I was doing transactions which will appear in my account because that real account was connected with the fraudulent Crypto account which is called myexpert100.com.

It is being said that this means that after I gave instructions to withdraw funds from Crypto.com, following the advice of the scammers, I could see the funds arriving at the fraudulent platform. I say, yes."[24]

[24] P. 301 - 302

At the hearing of 01 September 2025, the Service Provider FDAX presented their evidence in the person of Julian Yeung who stated:

"***We can see that the Complainant carried out a series of transactions involving the withdrawal and purchase, firstly, and then the subsequent withdrawal of Ethereum on his Crypto.com App account.***

There are a number of transactions that took place between 2 December 2024 and 9 December 2024 totalling to roughly 14.85 ETH.

From the Complainant's own evidence and his own testimony, we can see that all of these transactions were authorised by himself allegedly in concert with some third parties who were instructing him how to carry out these transactions.

And for the purposes of the Terms and Conditions as well as what was able to be seen by Crypto.com, these transactions were all authorised by the Complainant himself.

The withdrawals all went to the same external wallet, a wallet which is not operated by Crypto.com and for which we do not have any external information as to the account holders.

Based on that alone, we would say that Crypto.com bears no responsibility and Foris DAX MT bears no responsibility for what happens after these transfers are carried out in concert and in compliance with the Complainant's own instructions.

It is also important for us to note that the Complainant has confirmed that he was in control of his account at the time; he carried out those transactions based on the advice from these third parties but, nonetheless, it was his decision to carry out these transactions.

We will also say that throughout the process of the withdrawals, there were many warnings which are given to users when they make withdrawals to non-custodial wallets or wallets not hosted by Crypto.com.

First there is a warning that the withdrawal address is still in use, and that the withdrawal is to a trusted party; that they should not be easily misled by third parties' promises of high returns. And that same or similar warning was

reiterated at each and every withdrawal upon making the withdrawal subject (?). There are references to various materials and tools hosted on Crypto.com's webpages, instructing, advising and educating users as to the nature of common scams as well as warning them that transactions to these third-party wallets are immutable and irreversible.

These are warnings that appear at the time of transactions but the same is repeated in the Terms and Conditions supplement.

Given that these transactions were not filed (?) to us at the time they were made, given that the Complainant himself did not realise that these transactions were fraudulent ones until a week after the last transaction was made based on our records.

Our case is that Foris DAX MT bears no responsibility for the withdrawals that we carried out in compliance with the Complainant's instructions."[25]

Complainant did not conduct a cross-examination of the evidence by 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.

[25] P. 543 - 544

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

Further Considerations

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

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

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

- 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 after the last of the disputed transactions was already executed and finalised.[27]

  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).[28]

  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 …".[29]

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

[27] 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).
[28] E.G. https://www.chargebackgurus.com/blog/chargebacks-more-volatile-complex-than-cryptocurrency
[29] P. 511 - 512

any specific regulatory requirements applicable to it, nor did he find any infringement of the Terms and Conditions applicable in respect to the service offered.

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

i. AML/ CFT Framework

Further to the Prevention of Money Laundering Act (Cap. 373) and Prevention of Money Laundering and Funding of Terrorism Regulations ('PMLFTR'), the Financial Intelligence Analysis Unit (FIAU) issued Implementing Procedures including on the *'Application of Anti-Money Laundering and Countering the Funding of Terrorism Obligations to the Virtual Financial Assets Sector'*.[30]

These are *'sector-specific Implementing Procedures [which] complement the Implementing Procedures – Part I [issued by FIAU] and are to be read in conjunction therewith'*.[31] 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[32] and Travel Rule[33] obligations which entered into force in 2025, and which give more

[30] https://fiaumalta.org/app/uploads/2020/09/20200918_IPsII_VFAs.pdf
[31] 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'*
[32] EU Directive 2023/1114 on markets in crypto assets https://eur-lex.europa.eu/legal-content/EN/AUTO/?uri=celex:32023R1114
[33] 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

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[34] 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),[35] for the devise of enhanced mechanisms to mitigate the occurrence of customers falling victims to such scams.

Furthermore, in the Arbiter's decisions of recent months there is a recommendation that VASPs should enhance their on-boarding processes where retail customers are concerned warning them that custodial wallets may be used by scammers promoting get-rich-quick schemes as a route to empty the bank

https://www.eba.europa.eu/sites/default/files/2024-07/6de6e9b9-0ed9-49cd-985d-c0834b5b4356/Travel%20Rule%20Guidelines.pdf

[34] *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

[35] Such as Case ASF 158/2021

accounts of retail customers and disappear such funds in the complex web of blockchain anonymous transactions.[36]

Compliance with such recommendations or lack thereof will be taken into consideration in future complaint adjudications."[37]

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."[38]

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****;…"*[39]

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

[36] Such as Case ASF 069/2024
[37] Emphasis added by the Arbiter
[38] Emphasis added by the Arbiter
[39] 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 one week when the fraudulent transfers were happening in relatively consistent quantity values in funds transferred from Complainant's account with banks in Latvia.

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* existed at the time of the disputed transactions. An EU regulatory framework was only recently implemented effective for the first time in this field in 2025.[40]

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.

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

[40] 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/

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.[41]

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 Servces Malta Ltd (OPENPAYD - SP 1)

The case against OpenPayd is based on the assumption that the Complainant had an account with OpenPayd given that all the transfers from his Bank in Latvia indicated himself as beneficiary in an IBAN account with OpenPayd.

He explained that:

"Fraudsters gave him a bank account with OpenPayd ... telling him that this account ... is in his name. He made several transfers to his bank account putting the beneficiary's name as himself in that bank account. When he understood that he was defrauded, the money which was transferred from Citadele Banka sent a request to OpenPayd … to return the funds since the transfers were fraudulent. The answer was that (he) was not a client of that account and that means that the origin of the money was not checked, and that the beneficiary's name was not compared to the account number to which the money was transferred."[42]

The preliminary plea of non-competence and the non-application of contumacy rules have already been dealt with earlier in this decision so the Arbiter will proceed to consider the merits of this complaint against OpenPayd.

[41] 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

[42] P. 88

The first hearing on the merits was held on 27 May 2025, where the Complainant, on being cross-examined on the evidence quoted above, stated:

"I am a director of a company which produces vitamin ???

I am referred to page 3, fourth line, of my complaint where I wrote:

'However, I was somehow redirected to move to another platform that turned out to be a part of an investment scam.'

Asked to give some information on how this happened, I say that I did not have the Crypto.com platform. I did not see the Crypto.com platform as I did not know that I needed to check that. I just had the Crypto Wallet opened with Crypto.com and then the scammers said that I could see that I bought USDT on the platform, myexpert100.com. I saw all the transactions in myexpert100.com which appeared to be a fraudulent platform.

I say, yes, the transfers originated from Citadele Banka.

It is being stated that earlier I said that the fraudsters gave me a bank account in my name.

Yes, they opened an account with OpenPayd Financial Services, and it was in my name. I also asked again what I should put as beneficiary's name and they said that I should put my name as beneficiary.

Asked whether when I refer to the fraudsters would I be referring to Mr Piotr Nikonowicz, I say that Mr Nikonowicz told me to sign the deposit statements which were issued to the scammer but the contact person that I had communicated with was Dmitri Bosnia.

So, yes, when I am referring to the scammers, I am referring to one or both of these people.

Asked when the fraudsters told me that a bank account was opened in my name whether I checked that this is correct and whether I received anything, I say I trusted them that this bank account was in my name, and I did not see any statements confirming this.

I say I knew that I had never opened a bank account with OpenPayd but that bank account was opened when I opened a Crypto Wallet with the help of scammers and, therefore, I trusted that that bank account was connected to my Crypto Wallet.

I say that before this event, I had never contacted OpenPayd for a service.

Asked whether I filed a complaint with Citadele Banka about these transfers, I say, yes, I have submitted a complaint with Citadele Banka requesting the return of those transactions and the bank replied that they have received from OpenPayd that there is no money in the account to which the transactions were made, therefore, the return is not possible.

The Arbiter intervenes to ask for clarification whether a complaint was made with the bank or whether a request for chargeback was made to the bank.

I say that there was a request to recall the funds. No, there was no complaint.

In my complaint I mentioned that there were two withdrawals of funds and asked whether this means that of the total amount I transferred, there was an amount which I received back, I say, yes, that is correct. There were two withdrawals of funds which I received at the end in my bank account and those were transferred from the account of OpenPayd which initially I made transfers to. The account number was the same.

I confirm that the last two documents attached to my complaint (p. 52 and p. 53) are the two withdrawals I was referring to. One was for 1 500 USDT (€1,393,14) and the other one for 50,00 USDT (€46.46).

I confirm that these were received in my account at Citadele Banka. I confirm that the payer was OpenPayd."[43]

The second hearing held on 01 September 2025 was for the evidence of the Service Provider who presented an affidavit[44] prepared by their Operations Manager, Ms Jessica Micallef. This broadly repeated the explanation which was made in their official reply[45] that:

"OpenPayd is a provider of payment services registered in Malta under company registration number C75580 and is licensed and regulated by the Malta Financial Services Authority as a financial institution in terms of the Financial Institutions Act (Chapter 376, Laws of Malta). As you will be aware, OpenPayd is not and has never made itself out to be a bank or provider of investment services. OpenPayd

[43] P. 88 - 90
[44] P. 113 - 116
[45] P. 77 - 80

provides payment services to its corporate clients (inter alia the Merchants) in order to assist them in their own reconciliation of payments.

Please note that the letter included in the Complaint suggests that the payments made from the Complainant's bank account and paid to Crypto.com (as purportedly instructed by www.myexpert100.com's representatives) were paid to a 'bank account' to OpenPayd. This is not an accurate description of our services – funds were received by OpenPayd as receiving Payment Service Provider (PSP) for its merchant Crypto.com.

OpenPayd reiterates that it has never had any commercial or contractual relationship with the platform www.myexpert100.com and its representative(s) who may or may not have separately engaged with the Complainant. In this, OpenPayd is not aware, nor could have been or ought to have been aware, of any arrangement between the online platform www.myexpert100.com and its representatives, the Merchant and the Complainant.

With respect to the allegations of improper onboarding and collection of documentation, in terms of law, OpenPayd is to carry out customer due diligence on its customer, Crypto.com, both at onboarding stage and during their relationship as required by applicable laws and regulations. It is not incumbent on OpenPayd as a PSP to carry out KYC/CDD checks on the customers of its merchants as in terms of law, there is no legal relationship between the merchant's customers and OpenPayd. Accordingly, customer due diligence requirements concerning all Crypto.com customers are to be performed by Crypto.com and not by OpenPayd.

It appears this case relates to an unfortunate incident of fraud in the Complainant's regard which is altogether distinct from the tools that are to be adopted as mandated at law for the purposes of prevention of money laundering and financing of terrorism. Ultimately, it is incumbent on the merchant to adopt such measures in regard to its customers such as the Complainant, and on OpenPayd vis-à-vis its merchants. In this respect, OpenPayd has always complied with its statutory obligations in implementing the required measures for the prevention of money laundering and financing of terrorism.

… …

On the Complainant's specific points raised in their letter to the Arbiter, we wish to make clear that:

- *OpenPayd has no legal relationship with the Complainant.*
- *OpenPayd has no relationship whatsoever with the unknown account manager(s) at the online platform 'https://myexpert100.com/', and OpenPayd has had no involvement in any of the interactions that the Complainant has chosen to have with the representative(s) of the online platform 'https://myexpert100.com'.*
- *In respect of the request to return funds which the Complainant authorised to be paid from their third-party bank account, the Complainant should address this request to Crypto.com as a beneficiary of those payments."*[46]

In her affidavit, Ms Micallef explained how the VIBAN system works to credit the funds to the VIBAN account holder, even if the beneficiary named in the transfer is different from the VIBAN account holder.[47]

During cross-examination on her affidavit, Ms Micallef stated:

"***Asked when we receive a payment order where the name of the beneficiary on the payment order and the beneficiary of the IBAN are different whether we move on by the IBAN number and neglect the beneficiary on the payment order, I say that the name wouldn't have been different than the beneficiary in this case. They would be linked to Foris's account as a separate virtual IBAN.***

It is being said that this is not true because the complainant has submitted a payment order where it clearly shows the beneficiary and the IBAN number is not the same.

It is being said that if you receive a payment order and the beneficiary is Mr X, but the IBAN number belongs to somebody else, we credit the amount to the IBAN number. I say, yes, unless there would have been any flags on the name or flags on the specific payment, the payment will be credited."[48]

[46] P. 79 - 80
[47] P. 115
[48] P. 110 - 111

Analysis and Observations

To avoid repetition, the Arbiter refers to proceedings of case ASF 155/2024 which relates to the same 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.

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 a director of a company producing XXX,[49] 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.[50] It is greed that was forcing the Complainant to continue transferring funds to the scammers, many of them under the false pretence of payment of taxes to enable encashment of the fictitious profits.[51]

The Complainant, by his own admission, knew that whilst the funds were being transferred to what he believed was a personal account with OpenPayd, the final destination of these funds were to his investment platform 'myexpert100.com' through Crypto.com.

"I knew that I had never opened a bank account with OpenPayd but that bank account was opened when I opened a Crypto Wallet with the help of the scammers and, therefore, I trusted that that bank account was connected to my Crypto Wallet."[52]

In reply to a question by the Arbiter whether he knew that although he put his name as beneficiary in the payments orders, he knew that the money was going to Crypto.com, Complainant confirmed:

[49] P. 88
[50] P. 40
[51] P. 25; 29; 31
[52] P. 89

"I was thinking that the money was going to his (my) ***opened account with Crypto.com."***[53]

He also stated:

"I thought that I was doing transactions which will appear in my account because that real account was connected with the fraudulent Crypto account which is called myexpert100.com.

It is being said that this means that after I gave instructions to withdraw funds from my Crypto.com, following advice of the scammers, I could see the funds arriving at the fraudulent platform, I say, yes".[54]

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 as above indicated, leaves no doubt in Arbiter's mind that the loss incurred by the Complainant was caused by his greed and 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.

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

[53] P. 111
[54] P. 302

All decisions regarding this complaint are without prejudice to the potential rights that may be explored against his home bank who under the PSD 2,[55] have a much more 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. No evidence was forthcoming that Complainant has lodged such formal complaint with his home bank other than requested recalls which were unsuccessful.

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.

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

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.
