

Before the Arbiter for Financial Services

Case ASF 090/2023

AI (The Complainant)

vs

Foris DAX MT Limited (C 88392)
(The Service Provider/Foris DAX)

Sitting of 07 February 2024

The Arbiter,

Having seen **the Complaint** dated 18 July 2023¹ relating to the Service Provider's alleged failure to:

*"provide information it should have collected according to FATF travel rule requirement (Recommendation 16) ... assumingly, it has also failed to collect it upon any of the transactions made by the Complainant."*²

The Complaint

The Complainant, through his lawyers Petrova Law Firm/Legal Service Agency based in Bulgaria, admits that:

"In particular, Client was defrauded by unknown persons operating through the unlicensed financial brokerage platform www.brokeragea.com, which solicited the Client to invest substantial amount of money. All payments were made in the way of crypto-transactions to wallets nominated as beneficiary wallets by the representatives of the unlicensed financial broker. All such transfers were made through the Client's wallet hosted by Crypto.com.

¹ Page (p.) 1 – 6 and attachments p. 7 -31

² P. 3

We consider the beneficiary wallets being an integral part of the fraudulent scheme behind www.brokeragea.com. We also know that under the so-called travel rule, virtual assets services providers (VASP) are put under certain obligations, which include collection and keeping record of information about the beneficiary wallets, especially about if the beneficiary wallet is hosted (including which is the hosting exchange) and/or if the beneficiary wallet is unhosted.

Client's Request to Crypto.com

*Based upon the understanding that **Crypto.com** is acting complaint and will provide the due care towards its own wallet-holders (such as **AI**), we have sent a relevant request for provision of information (Attachment ./02) – Letter of Demand to Crypto.com). Such letter was solely based upon the assumption that*

- (a) **Crypto.com** should have collected the requested information as a part of their regulatory obligations **(if it has acted FATF complaint as it declares and advertises)**;*
- (b) Neither part of the requested information requested is considered confidential and is not protected under any law **(it does not qualify under any rules as personal information)**; and*
- (c) Client has **justified legal interest** to have knowledge about the beneficiary wallet holder and about the crypto-exchanges that possibly hosted wallets, to which Client made transactions.*

*As a matter of fact, said letter is requesting information ONLY about the name of the beneficiary person and the location (hosting entities) of the beneficiary wallets, where the client has transferred Crypto from the Client's Crypto.com hosted wallet. It is based upon the travel rule requirements imposed on VASPs by **FATF'S UPDATED GUIDANCE FOR A RISK-BASED APPROACH/VIRTUAL ASSETS AND VIRTUAL ASSET SERVICE PROVIDERS** (V. 2021). With slight deviations in the thresholds and the required information to be recorded, similar regulations are adopted by **Moneyval, FINCEN and FINTRAC**.*

It shall be noted with this regard, that according to Section 179 of the FATF Guidance for a Risk Based Approach (which is the general rule) the requirements of Recommendation 16 apply to VASPs whenever their

*transactions, whether in fiat currency or VA, involve: (a) a traditional wire transfer, (b) a VA transfer between a VASP and another obliged entity (e.g. between two VASPs or between a VASP and another obliged entity, such as a bank or other FI), or (c) a VA transfer between a VASP and a non-obliged entity (i.e., an unhosted wallet)."*³

It was further argued that:

*"where the counter-party is a non-obliged entity (i.e. unhosted wallet), VASP⁴s are still under certain AML/CFT and fraud prevention monitoring and control measures (sections 203 and 204 of the FATF Guidance for Risk Based Approach, which also include feasible effort to collect information in the above described scope."*⁵

In particular, the Complainant was seeking information from the Service Provider as follows:

- 1) *'Full record of the transactions made by the Client to the beneficiary e-wallets nominated by www.brokeragea.com;*
- 2) *Full record of the information that you should have recorded under the 'travel rule' for the below beneficiary e-wallets whether hosted by obliged entities or unhosted:*
 - *Ox9ce6154C262c31a6ACF045CF023726e41B07D5FE*
 - *OxC1aF881cd838634002F63C73e9Eee2AA7D9B27f9*
- 3) *Where the beneficiary e-wallet is unhosted, full record of the AML and fraud prevention measure including risk related information to the Client;*
- 4) *Were personal data of the Client ever provided to third party/parties and (if so) on what legal grounds?*
- 5) *Which is the legal entity providing wallet to the Client, respectively – where (under which jurisdiction) is this legal entity regulated?'*⁶

³ P. 21 -22

⁴ Virtual Asset Service Providers

⁵ P. 9

⁶ P. 10

The Complainant argued that failure of the Service Provider to provide the requested information affected his chances for successful recovery and sought compensation for the (fiat currency) equivalent of USDT⁷ 266,470.

Service Provider's reply

The Service Provider had replied on 20 April 2023 to the direct complaint filed with them by the Complainant arguing that all payments were authorised by the Complainant and that according to their Terms and Conditions, they refuted any claim for compensation. They also added:

"All transactions done on blockchain are immutable, and as such it is not possible for Crypto.com to revoke such transactions.

As your Client appears to have been defrauded by a third party, your Client should consider notifying the local authorities who will request any information you seek through the proper channels should they choose to do so and if applicable.

For any third-party requests in relation to any accounts purported to be maintained by us, we will act upon being served by a Court Order from a Court with the appropriate jurisdiction".⁸

They also informed that a statement of the transactions was available on their App online and can be downloaded. They also denied having any affiliation with www.brokeragea.com.

In Foris Dax's official reply to the complaint filed on 27 July 2023⁹ with the Office of the Arbiter (OAFS), they stated:

- *'Foris DAX MT Limited (the "Company") offers the following services: a crypto custodial wallet (the "Wallet"), the purchase and sale of digital assets on own account, and 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) for the purposes of investing in crypto assets. Services are offered through the Crypto.com App (the "App"). The*

⁷ Tether (USDT) is a cryptocurrency with a value meant to mirror the value of the U.S. dollar.

⁸ P. 19

⁹ p. 37 – 46 and attachments p. 47 -58

Wallet is only accessible through the App, and the latter is only accessible via a mobile device.

- *AI (the “Complainant”), e-mail address: XXXXXXXXXX@gmail.com became a customer of Foris DAX MT Limited through the Crypto.com App and was approved to use the Wallet on December 14, 2021.”¹⁰*

They also gave a detailed explanation of the transactions being the subject of this complaint that happened between 25 January 2022 and 27 July 2022 spread over 7 transfers to 2 different unknown external wallets involving USDT 275,345.

Service Provider maintained that Complainant was solely responsible for the security and authenticity of all instructions submitted through his Wallet as outlined in the Terms of Use and quoted article 7.2 Digital Asset Transfers:

“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.”¹¹

The Hearings

The first hearing was held on 06 November 2023, where the Complainant failed to attend or connect, and was represented by Ms Mariya Dyulgerova from the Bulgarian law firm representing him.

¹⁰ P. 37

¹¹ P. 46

She stressed that:

“our complaint is not about compensation. It is about requesting information about the Wallets that have been transferred to Crypto. ...

We were seeking this information from Crypto.com but we did not receive it. That is why we have filed a complaint with the OAFS.”¹²

As the Complainant was not attending and declined even to make written submissions in case he had language problems to communicate verbally, no cross-examination was possible. The Complainant’s legal representative insisted on proceeding to the proofs of the Service Provider without offering possibility for cross-examination of the Complainant.

A second hearing was held on 15 December 2023 where, again, the Complainant failed to attend or connect, and was represented by his legal assistance.

The Service Provider requested dismissal of the Complaint. The Arbiter ordered continuation of hearing for proofs of the Service Provider but stated that he will bear in mind the impossibility of cross-examining the Complainant in adjudicating this complaint.

The Service Provider stated that they rest on their official reply to the Complaint and have no further proofs.

Final Submissions

Complainant’s legal assistant declined to make or file any final submissions.

The Service Provider agreed to make final submissions and the Arbiter requested that in their submissions, they address the deemed obligations that Complainant had raised under FATF Recommendation 16 (Travel Rule) and, also, give reassurances that their monitoring systems comply with Section 2.3 of FIAU’s implementing procedures for Virtual Financial Asset Sector.

In their final submissions filed on 31 January 2024,¹³ Foris DAX MT obliged the requests of the Arbiter stating:

¹² P. 59

¹³ P. 97 - 102

'The Arbiter has asked the Respondent to address the obligations of the Respondent under the FATF 16 ("Recommendation 16"). It ought to be stressed that Recommendation 16 is, as titled, a recommendation. These are guidelines, rather than a regulation or a law. Whilst there are wider discussions to incorporate this rule as part of the "Markets in Crypto Regulation" (MiCA), this is not expected to form part of the law until 2025 to allow regulators in the region to better understand how to apply this in practical terms. Accordingly, there are yet to be any detailed guideline on how Recommendation 16 ought to be implemented by service providers.

In fact there are real concerns that the implementation of Recommendation 16, without the proper safeguards, will likely conflict with the general duties on data privacy, as it requires the sharing of personal data between VASPs, particularly when the FATF has yet to prescribe a specific method or technology for sharing data at this time.

In any case, it is highlighted that Recommendation 16 merely recommends that in the instance where transactions occur between users of VASPs, these VASPs should consider gathering and exchanging real-name user information with one another and to make this information available to appropriate authorities upon request.

*Recommendation 16 was developed with the objective of preventing persons from having unfettered access to electronic transfer services for moving their funds, and for detecting such misuse when it occurs. To this end, this recommendation requires service providers to transmit, together with the funds, information on the originator and the beneficiary of the funds' transfer which is being implemented with respect to banking transactions. It must be stressed that the current discussions revolve around introducing this to transfers of virtual financial assets **provided that both the sender and recipient wallets are custodial wallets – i.e., wallets which are held on recognised (and likely licensed) exchanges.** It is not the case here. The transfer by the Complainant was done to a non-custodial wallet and therefore, it is not possible nor does the recommendation oblige the service provider to obtain such information.*

Custodial wallets are those provided by centralised crypto exchanges like Crypto.com or other providers. Users initiate a transaction through the platform of the exchange who in turn provide the users with the key. Therefore, in so far as collecting and holding or transferring information, provided this is from a custodial wallet held on an exchange to another custodial wallet, the data collection is possible. With non-custodial wallets, the holder is the user directly, and the user has complete control over the key along with the funds without any involvement of a third-party platform provider. In this case, the Recommendation 16 does not oblige the collection of such data as this is not possible.

Furthermore, respectfully, whilst the Respondent is absolutely committed to carrying out its obligations and has adhered to its regulatory obligations, including and in particular those relating to Money Laundering and Financing of Terrorism, the implementation of such obligations is a matter pertaining to the competent regulators to determine. It is humbly submitted that the Arbiter does not have competence to determine whether the Respondent has implemented and carried out its obligations in terms of law pertaining to measures to combat the financing of terrorism and commissioning of Money Laundering.

If for the sake of argument, which is denied, the Recommendation, which again does not have the force of law, is not being implemented by the Respondent, this would if at all, be a matter for which the regulator authority has the competence to assess following a thorough assessment of its measures after having undertaken a compliance visit and audit. This is not the purpose and scope of the complaint and would seem that the Complainant has misdirected its complaint to the Respondent when it ought to have done so against the unnamed third party that purportedly advised him to transfer his assets to a non-custodial wallet.¹⁴

'Section 2.3 FIAU Implementing Procedures

The Respondent is licensed by the Malta Financial Services Authority ("MFSA") as a VFA Respondent as per the MFSA's Financial Services Register

¹⁴ P. 99 - 100

and holds a Class 3 VFAA licence granted by the MFSA under the Virtual Financial Assets Act, 2018 (“VFAA”).

*The Respondent submits that the internal monitoring procedures of the Respondent are fully in line with the requirements as required under the FIAU Implementing Procedures. In actual fact, and to further support paragraphs 22 et seq. above, Section 2.3 of Part II of the FIAU’s Implementing Procedures likewise provides that “the name of the institution holding” the assets is to be collected and retained “**in the case of custodial wallets**” (emphasis added).*

As provided above, this does not apply to this case. So much so, the Implementing Procedures provide that “To the extent that this may be possible” (page 21) the Respondent to implement the measures provided therein, thereby acknowledging that of its very nature, much depending on the type of wallet, this is not always possible.

The Respondent would first highlight that the Respondent is fully compliant under the AML, CFT and KYC laws and regulations that the Respondent is subject to, including the Prevention of Money Laundering and Funding of Terrorism. This includes comprehensive internal monitoring, account monitoring and external reporting procedures.

In respect of transaction monitoring as it relates to the Disputed Transactions, it is submitted that the Respondent has carried out due monitoring of these transactions as they were performed. However, due to its overarching obligations due to the FIAU in respect of transaction reporting, the Respondent is not at liberty to share details of the internal monitoring results for any individual cases.¹⁵

Having heard the parties

Having seen all the documents

Considers

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

¹⁵ P. 101

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

Furthermore, it was not clear what remedy the Complainant actually was seeking. Whilst in his official complaint filed with the OAFS, he sought compensation for the bulk of his loss on the pretext that failure by the Service Provider to provide the information sought had prejudiced his chances of recovery, during the hearings his legal representative stated that their complaint was not about compensation but about obtaining the information requested.

The Arbiter fully shares the view expressed by the Service Provider in their final submissions that FATF Recommendation 16 does not (so far) amount to an obligation to keep and/or make available the information sought by the Complainant.

The Arbiter also notes the Service Provider's affirmation that they fully comply with AML, CFT and KYC laws and regulations under the Prevention of Money Laundering and Financing of Terrorism obligations. In so doing, the Arbiter affirms that it is not the competent authority to adjudge and consider any infringements to such rules and regulations, and any complaints on such matters should be addressed to the FIAU as Malta's competent authority in terms of Chapter 373 of the Laws of Malta.

Applicable Regulatory Framework

Foris DAX is the holder of a Class 3 VFSA licence granted by the Malta Financial Services Authority ('MFSA') under the Virtual Financial Assets Act, 2018 ('VFSA').

Apart from the relevant provisions under the VFSA, and the *Virtual Financial Assets Regulations, 2018 (L.N. 357 of 2018)* issued under the same act, Foris DAX is also subject to the rules outlined in the Virtual Financial Assets Rulebook ("the VFA Rulebook") issued by the MFSA. The said rulebook complements the VFSA 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*”¹⁶ applicable to its licence holders (including under the Virtual Financial Assets) titled “*Guidance on Technology Arrangements, ICT and Security Risk Management, and Outsourcing Arrangements*” (“the Guidance”).

Further Considerations

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

This is particularly so when taking into consideration various factors, including, the nature of the complaint, activities involved, and the alleged shortfalls as further detailed below:

- The Complaint involves a series of payments made by the Complainant from his account held with Foris DAX to 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 transaction 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

¹⁶ Guidance 1.1.2, Title 1, 'Scope and Application' of the 'Guidance on Technology Arrangements, ICT and Security Risk Management, and Outsourcing Arrangements'.

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

- Furthermore, it has not been demonstrated nor emerged that the alleged fraudster, to whom the payment was made by the Complainant, was another *Crypto.com* App user and, thus, a client of the Service Provider in the first place. The transfer was rather indicated to have been done to an “*external wallet*” and hence the Service Provider had no information about the third party to whom the Complainant was transferring his crypto.
- The Complainant seems to have only contacted the Service Provider on 17 March 2023, nearly 8 months after the last of the disputed transactions was already executed and finalised.¹⁷

Once finalised, the crypto cannot be transferred or reversed as specified in the Service Provider's Terms and Conditions of Use (and as typically indicated on various other internet sites).¹⁸

Once a transaction is complete and, accordingly, is not in a pending state, the crypto transaction cannot be cancelled or reversed by the Service Provider as provided for and warned in the Terms and Conditions of Foris DAX.

As indicated by the Service Provider, Clause 7.2(b) of its Terms and Conditions regarding the use of the *Crypto.com* App Services specifies that:

*“Crypto.com processes all Digital Asset Transfers according to the Instructions received from you and does not guarantee the identity of any recipient. You should verify all transaction information prior to submitting Instructions for a Digital Asset Transfer to Crypto.com as the Digital Asset Transfer may not be cancelled or reversed once processed ...”*¹⁹

¹⁷ 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).

¹⁸ E.G. <https://www.chargebackgurus.com/blog/chargebacks-more-volatile-complex-than-cryptocurrency>

¹⁹ P. 78

It is also noted that Clause 7.2(d) of the said Terms and Conditions which deals with *'Digital Asset Transfers'* further warns a customer about the following:²⁰

'We have no control over, or liability for, the delivery, quality, safety, legality or any other aspect of any goods or services that you may purchase or sell to or from a third party. We are not responsible for ensuring that a third-party buyer or seller you transact with will complete the transaction or is authorised to do so. If you experience a problem with any goods or services purchased from, or sold to, a third party using Digital Assets transferred from your Digital Asset Wallet, or if you have a dispute with such third party, you should resolve the dispute directly with that third party.'

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.

It is clear that the Complainant has, unfortunately, fallen victim of a scam done by a third party and no evidence resulted that this third party 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. A

²⁰ p. 79

regulatory framework is still yet to be implemented for the first time in this field within the EU.²¹

Whilst this area of business remains 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 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.²²

Decision

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.

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

²¹ 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 is expected to enter into force in 2025 – <https://www.financemagnates.com/cryptocurrency/can-mica-take-europe-to-the-crypto-promised-land/>

²² https://www.eiopa.europa.eu/document-library/other-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

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

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

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

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

The Arbiter considers that much more needs to be done on this front, apart from in other areas, to better protect consumers.

Service providers operating in this field need to also do their part and actively work to improve their onboarding process by evaluating the much-needed knowledge of benefits and risks for consumers who opt to venture into this field.²³

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

Alfred Mifsud
Arbiter for Financial Services

²³ It would not be amiss if at onboarding stage, retail customers are informed of typical fraud cases involving crypto asset transfers and warned against get rich quick schemes.

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.
