



MALTA

QORTI TAL-APPELL
(Sede Inferjuri)

ONOR. IMĦALLEF
LAWRENCE MINTOFF

Seduta tat-23 ta' Ottubru, 2024

Appell Inferjuri Numru 23/2024 LM

Yaniv Cohen (Detentur tal-Passaport Iżraeljan Numru 36943092)
(l-appellant')

vs.

FORIS DAX MT Limited (C 88392)
(l-appellata')

Il-Qorti,

Preliminari

1. Dan huwa appell magħmul mir-rikorrent **Yaniv Cohen (Detentur tal-Passaport Iżraeljan Numru 36943092)** [minn issa 'l quddiem 'l-appellant'] mid-deċiżjoni tal-Arbitru għas-Servizzi Finanzjarji [minn issa 'l quddiem 'l-Arbitru'] mogħtija fit-22 ta' Marzu, 2024, [minn issa 'l quddiem 'id-deċiżjoni appellata'], li permezz tagħha ddecieda l-ilment tiegħu fil-konfront tas-soċjetà intimata

FORIS DAX MT Limited (C 88392) [minn issa 'l quddiem 'is-soċjetà appellata'],
billi ddikjara kif ġej:

“Decision

The Arbiter sympathises with the Complainant for the ordeal he 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.

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 retail consumers may 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. (fn. 41: 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).

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

Fatti

2. Il-fatti tal-każ odjern jirrigwardaw kont li l-appellant fetaħ mas-soċjetà appellata fis-17 ta’ Novembru, 2022. Bejn is-17 ta’ Novembru, 2022, u l-20 ta’ Diċembru, 2022, huwa kien għamel ħamsa u għoxrin tranzazzjoni fil-munita *fiat* mill-kont bankarju tiegħu ġewwa l-Iżrael għall-munita lokali. Il-munita *fiat* kienet ġiet ikkonvertita għal *USDT stable coins*, u dawn ġew trasferiti għal tliet kartieri esterni, sabiex b’hekk l-appellant b’kollox ittrasferixxa USDT 200,795.02 ekwivalenti llum għal USD 200,000.

Mertu

3. L-appellant ippreżenta l-ilment tiegħu quddiem l-Arbitru fit-22 ta’ Awwissu, 2023, fejn filwaqt li sostna li (a) is-soċjetà appellata kellha tkun taf li huwa ma kellux l-esperjenza relattiva, u l-frekwenza u l-ammonti rispettivi tat-tranzazzjonijiet kellhom ikunu indikattivi tal-possibbiltà ta’ frodi; (b) huwa kien ilu f’kuntatt regolari mat-tim tal-*customer service* tas-soċjetà appellata sa minn meta għamel it-tranzazzjonijiet in kwistjoni, u dan it-tim qatt ma ħareġ xi twissija; (ċ) is-soċjetà appellata naqset milli tikkopera miegħu u mal-Awtoritajiet Iżraeljani li kienu qegħdin jinvestigaw il-frodi, u naqset milli tgħaddi d-debita informazzjoni li setgħet wasslet sabiex jiġu identifikati l-frodisti, u jiġu rkuprati l-flus misruqa; u (d) is-soċjetà appellata naqset milli tħares l-obbligi tagħha taħt il-liġi, u b’hekk dan wassal sabiex ma jinkixifx il-frodi fiż-żmien opportun u b’hekk jiġi minimizzat it-telf. L-appellant issottometta li huwa kien qiegħed jippretendi kumpens ta’ madwar USD 100,000.

4. Is-soċjetà appellata wiegħbet fil-15 ta' Settembru, 2023, fejn sostniet li seta' kien il-każ li tassew l-appellant spiċċa vittma ta' *scam*, iżda hija ma setgħetx tinżamm responsabbli għall-għemil ta' terzi, jew tal-istruzzjonijiet li kien għamel l-appellant innifsu.

L-Appell

5. L-appellant ħass ruħu aggravat bid-deċiżjoni appellata tal-Arbitru, u fil-11 ta' April, 2024, intavola appell quddiem din il-Qorti, fejn qiegħed jitlobha sabiex:

"...jogħgħobha tħassar u tirrevoka d-deċiżjoni tal-Arbitru għas-Servizzi Finanzjari tat-22 ta' Marzu, 2024, u dan billi tilqa' it-talbiet tal-appellant u tiċċad id-difiża ta' FORIS, u dan ai termini tal-provvedimenti u modalitajiet kollha li din l-Onorabbli Qorti jidhrilha xierqa u opportuni fiċ-ċirkostanzi tal-każ.

L-ispejjeż taż-żewġ istanzi għandhom jithallsu mill-kumpannija appellata FORIS."

Jispjega li l-aggravju tiegħu huwa li l-Arbitru għamel interpretazzjoni żbaljata tal-fatti relattivi u tal-liġijiet applikabbli għall-każ odjern.

6. Is-soċjetà appellata wiegħbet fit-8 ta' Mejju, 2024, fejn sostniet li d-deċiżjoni appellata hija waħda ġusta, ekwa u legali, u għandha tiġi kkonfermata, u dan filwaqt li l-appell interpost għandu jiġi miċħud, bl-ispejjeż kontra l-appellant.

Konsiderazzjonijiet ta' din il-Qorti

7. Din il-Qorti ser tgħaddi sabiex tikkunsidra qabel xejn kwistjoni preliminari li qiegħda tiġi ssollewata mis-soċjetà appellata, li hija dik tan-nullità tal-appell

odjern, stante li l-appellant m'ottemporax ruġu mad-dispożizzjonijiet tal-para. (a) tas-subartikolu 180(1) tal-Kap. 12, fid-dawl tal-fatt li huwa mhux residenti hawn Malta.

8. Il-Qorti tgħid li s-socjetà appellata għandha raġun. Id-dispożizzjonijiet tal-para. (a) tas-subartikolu 180(1) tal-Kap. 12 huma ċari u inekwivoċi fl-intendiment tagħhom:

“180.(1) Bla ħsara tad-dispożizzjonijiet tal-artikolu 181, il-preżentata tal-iskritturi tista’ ssir –

(a) mill-parti stess li tidher fl-isem tagħha nfisha, ... jew bħala prokuratur ta’ persuni li jinsabu barra mill-Gżira ta’ Malta jew ta’ Għawdex, li fiha l-iskrittura tiġi ppreżentata;”

...

9. L-imsemmija dispożizzjonijiet ma jhallu l-ebda dubju li l-liġi ma tippermettix persuni li huma residenti barra minn dawn il-gżejjer, li jipprezentaw skritturi fir-Registru tal-Qorti, sakemm huma mhumix debitament rappreżentati fl-istess gżejjer. Fil-każ odjern l-indirizz li ndika l-appellant fir-rikors tal-appell tiegħu huwa ġewwa l-Iżrael, u għadarba ma jirrizultax mill-atti li huwa debitament rappreżentat hawn Malta skont il-liġi, dan ma setax għamli, u l-appell tiegħu huwa wieħed irregolari.

Decide

Għar-raġunijiet premessi l-Qorti tiddikjara l-appell odjern irritu u null u tastjeni milli tiegħu konjizzjoni tiegħu.

Bl-ispejjeż kontra l-appellant.

Moqrija.

Onor. Dr Lawrence Mintoff LL.D.
Imħallef

Rosemarie Calleja
Deputat Registratur



**QORTI TAL-APPELL
(SEDE INFERJURI)**

S.T.O. PRIM IMHALLEF MARK CHETCUTI

Illum l-Erbgha, 15 ta' Ottubru, 2025

Numru 1

Rikors Nru. 23/2024

Yaniv Cohen

vs

Foris Dax MT Limited

Il-Qorti,

Din hi sentenza minn appell ta' Yaniv Cohen wara decizjoni tal-Arbitru ghas-Servizzi Finanzjarji tat-22 ta' Marzu 2024 li fiha sab li s-socjeta Foris Dax MT ma kinitx responsabbli ghat-telf ta' flus sofferti minn Cohen in konnessjoni mas-servizz provdut mill-istess Foris Dax.

Rat in-noti.

Bhala fatti fil-qosor jirrizulta illi s-socjeta appellata hi service provider li tipprovdi crypto custodial wallets lil min jabbona maghha permezz tal-mobile application crypto.com. Permezz ta' din l-application il-klijent ikun jista' jitransferixxi assi digitali mill-kont tieghu li jigu tradotti fi crypto currency lit-terzi li gia ghandhom wallets mal-istess service provider jew f'dak li jissejjhu external wallets li jkun jaf bihom il-klijent biss. F'dan il-kaz jidher li l-appellant kien wasal f'arrangement ma' terzi bl-isem ta' 'Antrush Group Limited' li irrakomandawlu li

t-trasferiment lilhom tal-assi digitali jsir permezz ta' crypto.com. Jirrizulta li l-appellant gie accettat mis-socjeta Foris Dax li juza l-pjattaforma digitali taghha biex jaghmel it-trasferimenti li ried. Bejn Novembru u Dicembru 2022 ghamel 25 transazzjoni b'valur tal-USD200,000 lil tlett external wallets li ipprovdewlu 'Antrush Group Limited' u li wara irrizulta li din kienet skema frawdolenti ta' dawn it-terzi biex jiehdulu flusu. L-appellant isostni li Foris Dax bhala service provider kienu responsabbli ghal nuqqasijiet regolatorji li wassal biex sar dan il-qerq a spejjez tieghu u kelhom ihallsuh id-danni li soffra.

L-arbitru finanzjarju jghid hekk fid-decizjoni tieghu:

The Complaint

The Complainant opened an account with the Service Provider on 17 November 2022. Between 17 November 2022 and 20 December 2022, he carried out 25 transactions involving transfer of fiat currency from his bank account in Israel in local currency. The fiat currency was converted in USDT [Tether (USDT) is a stable coin pegged at 1-to-1 with a matching fiat currency and backed 100% by Tether's reserves] stable coins and these were regularly transferred to three external wallets so that in all Complainant transferred USDT 200,795.02 to such wallets. The counter value in US\$ today is about USD 200,000.

Complainant basically raises these issues:

- Service Provider should have realised that Complainant was inexperienced, and the frequency and size of the transfers should have alerted the Service Provider to detect the possibility of the Complainant being defrauded and should have intervened to alert him to such possibility.
- Complainant had been in regular contact with the customer service team of the Service Provider at the point of making the transfers and they never alerted him to anything not being in order.
- Service Provider failed to co-operate with the Complainant and with the Israeli Authorities, that were investigating the fraud, and failed to provide information which could have identified the fraudsters and help in recovery of the stolen funds.
- Service Provider has failed to meet its obligations under Anti Money Laundering and Finance of Terrorism regulations and such failure prevented early detection of the fraud which would have minimized the loss.

By way of compensation, Complainant was seeking around US\$100,000 [p. 4 - later revised specifically to US\$103.079 (P. 220)]. The figure was arrived at by taking into consideration transactions exceeding the threshold of €15,000 [The threshold of €15,000 is based on the definition of 'occasional transaction' in 2 (1) of Subsidiary Legislation 373.01 Prevention of Money Laundering and Funding of Terrorism Regulations] as well as other transactions which, by virtue of their high value, should have triggered due diligence alerts within Crypto.com operational protocol [p. 220].

Complainant argued that following the first transaction exceeding €15,000, there were other transactions involving €148,423 which could have been avoided if he had been informed and educated regarding the potential risks or unusual nature of these transactions [p. 217].

The Complainant presented a professional report [p. 69-90] he commissioned to T&H Consulting based in Hungary with a view to map the web of transactions of the funds he had transferred to the three external wallets and how these assets were moved subsequently.

This report identifies the scammers as 'Antrush Group Limited' with website aglvip.com. It confirms that the USDT were transferred over 25 transactions to three external wallets.

Subsequently, these funds were moved to other wallets as mapped in folio no. 89. There were 5 transactions involving payments of a cumulative, relatively small amount of USDT 2247.65 with the largest being USDT 1,139.43 and the smallest USDT 100. These were transactions effected between 21 November 2022 and 22 December 2022 and were made to wallets hosted by Crypto.com. Service Provider would have due diligence documents related to the owners of these accounts [p. 78].

Reply of Service Provider

In their reply of 15 September 2023, Service Provider explained that Foris DAX MT offers the following services:

'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 purpose of investing in crypto assets. Services are offered through the Crypto.com App (the "App"). The Wallet is only accessible through the App, and the later is only accessible via a mobile device.' [p. 100]

They gave a detailed sequence of the various transactions executed by the Complainant on his Wallet [p. 101-123].

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 Mr Cohen himself, and the Company was merely adhering to the Complainant's instructions and providing the technical service of transferring the requested assets to the address provided by him.

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 this address falls under the responsibility(ies) of the provider of said wallet.

Unfortunately, Crypto.com cannot revoke any virtual asset withdrawals because blockchain transactions are fast and immutable.

Mr Cohen 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 accepted by the Complainant for your reference:

QUOTE

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. Whilst we fully empathize with Mr Cohen in this regard, it cannot be overlooked that he had willingly, according to his statements, transferred his virtual asset holdings from his Crypto.com Wallet to external wallet addresses which he has no access to.

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 or the veracity of any third-party or (or the instructions received from the Complainant themselves.' [p. 123-124]

Observations & Conclusion

Summary of main aspects

The Complainant made a transfer of his digital assets (USDT) using the Crypto.com app. The said transfers were made to three different external wallet address allegedly used by fraudsters. The transfers were made on the specific instructions of the Complainant. External wallets are recognised only by their number and their proprietors or beneficial owners are not known to the transferor. The Service Provider has no obligation under current regulatory regime to keep or make available information relating to external wallets.

In essence, the Complainant is seeking compensation from Foris DAX for the Service Provider's failure to prevent, stop or reverse the payments he made to the fraudster.

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

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

Applicable Regulatory Framework

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

Apart from the relevant provisions under the VFAA, and the Virtual Financial Assets Regulations, 2018 (L.N. 357 of 2018) issued under the same act, Foris DAX is also subject to the rules outlined in the Virtual Financial Assets Rulebook ('the VFA Rulebook') issued by the MFSA. The said rulebook complements the VFAA by detailing *inter alia* ongoing obligations applicable for VFA Service Providers.

Chapter 3 of the VFA Rulebook specifically includes the rules applicable for VFA Service Providers which such providers must adhere to.

The Arbiter further notes that in the year 2020, the MFSA has also issued a 'harmonised baseline guidance on Technology Arrangements' [Guidance 1.1.2, Title 1, 'Scope and Application' of the 'Guidance on Technology Arrangements, ICT and Security Risk Management, and Outsourcing Arrangements' [Guidance 1.1.2, Title 1, 'Scope and Application' of the 'Guidance on Technology Arrangements, ICT and Security Risk Management, and Outsourcing Arrangements'] applicable to its licence holders (including under the Virtual Financial Assets) titled 'Guidance on Technology Arrangements, ICT and Security Risk Management, and Outsourcing Arrangements' ('the Guidance').

The FIAU [Malta's Financial Intelligence Analysis Unit being competent authority of AML issues] also issued Implementing Procedures on the Application of Anti-Money Laundering and Countering the Funding of Terrorism Obligations to the Virtual Financial Assets Sector [Layout 1 copy (fiaumalta.org)]. Section 2.3 of these Implementing Procedures detail the monitoring and transaction records obligations of VFA licensed entities.

Further Considerations

Having considered the particular circumstances of the case including the submissions made and evidence provided, the Arbiter considers that 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 external wallets 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 allegedly fraudulent external wallets causing a loss to the Complainant of approximately US\$ 200,000.

The Complainant expected the Service Provider to prevent or stop his transactions. He claimed that the Service Provider had an obligation to warn him of potential fraud.

The Arbitrator 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 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.

Furthermore, the Complainant must have himself 'whitelisted' the address giving all clear signal for the transfer to be executed. In fact, the Complainant himself did not raise any suspicion or evidence that there was any link between the Service Provider and the external wallet address he himself provided.

The Complainant seems to have only contacted the Service Provider after all alleged fraudulent transactions were executed.

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) [E.G. <https://www.chargebackgurus.com/btlog/chargebacks-more-volatile-complex-than-cryptocurrency>].

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 ...' [p. 191].

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: [*Ibid.*]

'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.'

Based on the facts presented during the case, the Arbitrator 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.

The regulatory regime applicable to a VFA Service Provider is different from and does not reflect the requirements and consumer protection measures applicable to banks and financial institution falling under EU regulatory regimes [Financial institutions based in Malta are regulated under a separate and distinct regulatory framework, namely the Financial Institutions Act (Cap. 376) which also covers the Payment Services Directive (PSD2), (Directive EU 2015/2366 on payment services in the internal market)].

Indeed, if the Complainant is seeking protection similar to that offered in the EU under PSD 2 obligations applicable to banks and payment institutions, he could seek advice on the appropriateness of seeking such protection from the Bank(s) that made the fiat currency transfers to his Crypto account.

It is probable that as he himself admitted, the Complainant has unfortunately fallen victim of a scam done by a third party and no evidence resulted that this third party was 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 regulatory framework is still yet to be implemented for the first time in this field within the EU [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/>].

Whilst this area of business remains unregulated in certain jurisdictions, other jurisdictions, like Malta, chose to regulate this field in the meantime to a home-grown national regulatory regime. While such regimes offer a certain amount of security to the consumer, since they are 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 [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].

The Arbiter notes that the Complainant makes a strong argument that the Service Provider has failed its AML obligations and, consequently, it has not triggered dutiful warnings to the Complainant to alert him to the possibility of his being scammed.

The Arbiter has no competence to investigate AML failures and any such claims should be directed to the competent authority in Malta, the FIAU, who have the competence and expertise to investigate such claims. The Arbiter, however, notes the strong assertions made by the Service Provider that they adhere to all AML obligations including the monitoring obligations imposed by Section 2.3 of the Implementing Procedures earlier referred to in this decision [p. 210].

The Arbiter also notes the assertion that the Service Provider's alleged failure to provide information to the Israeli Authorities has prejudiced the prospects of recovery of the funds stolen by the fraudsters.

The Arbiter cannot fault the Service Provider for insisting on adherence to their GDPR [General Data Protection Regulations — Regulation (EU) 2016/679] obligations which provides for disclosure of private information of third parties has to follow the proper process leading to authorisation as stipulated in the GDPR.

Furthermore, the supposition that disclosure of such information could have led to recovery is rather optimistic. Firstly, as explained, the Service Provider had no information on the owners of external wallets recipients of the alleged stolen funds. Secondly, as this particular case shows, even identification of the fraudsters (as is presumably done through the mapping report [p. 69 90] earlier referred to) does not necessarily lead to recovery.

However, the Arbiter is making a recommendation that could help the authorities to trace the connections of the fraudsters and at least limit their ability to perform further frauds.

Decision

The Arbiter sympathises with the Complainant for the ordeal he 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.

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 [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].

Yaniv Cohen appella minn din id-decizjoni. L-aggravji tieghu huma s-segwenti u ser jigu trattati wara xulxin.

L-ewwel aggravju

L-appellant isostni li l-arbitru applika hazin il-ligi ghal fatti. Isostni li l-artikolu 27 tal-Att dwar l-Attiv Finanzjarju Virtwali (Kap. 590) ighid li provveduri ta' servizzi finanzjarji jridu jagixxu b'mod onest u professjonali u jaderixxu mar-rekwiziti fl-

Att u ma kull obbligu iehor legali jew regolatorju, kif ukoll ikun soggett għall-obbligi fiducjarji skont il-Kap. 16 fejn applikabbli. Jghid li dan sehh għaliex ma ittehidx kont tar-regolamenti kontra l-Money Laundering u Finanzjar tat-Terrorizmu li bhala persuna soggetta, Foris Dax kellha tiehu kont u tiehu passi biex tevita kull riskju ta' money laundering li jirrizulta mill-attività kif ukoll tassikura li t-transazzjonijiet tal-klijenti tagħha huma konsistenti mill-gharfien tal-klijent u n-negozju tiegħu bir-riskji potenzjali kif ukoll is-sors tal-fondi tal-klijent. Jirriferi wkoll għall-implementing procedures in konnessjoni mas-settur tal-assi finanzjarji virtwali li jagħtu hjiel tas-sistema ta' verifiki necessarji meta jsiru pagamenti fosthom il-wallet address konness mal-pagament minhabba xi informazzjoni li tista' tinghata, li tuza mekkanizmu li jidentifikaw transazzjonijiet potenzjalment frawdolenti jew suspettuzi. In kwantu għal klijent tas-servizz, is-socjeta li magħha hemm din ir-relazzjoni għandha tiskrutinizza t-transazzjonijiet biex jigi assikurat li huma konsistenti mal-informazzjoni fuq il-klijent, n-negozju u profil ta' riskju tiegħu, u fejn jigi innotat transazzjonijiet anomali għal dak li solitament jagħmel il-klijent għandu jissinjala dan u jistabilixxi mnejn gejjien il-fondi. L-appellant ighid li Foris Dax naqset li twettaq due diligence għal kull transazzjoni minkejja li whud qabzu l-ammonti stipulati fir-regolament u minkejja li l-appellant ma kellux esperjenza u għamel 25 transazzjoni f'xahar. Jghid li t-Tribunal ma haditx kont ta' dan kollu minkejja li s-socjeta Foris Dax tagħti dettalji fuq transaction monitoring.

Is-socjeta appellata tirribatti dan l-aggravju b'diversi argumenti.

Il-Qorti ma issibx l-aggravju gustifikat. Ibda biex jingħad li l-appellant jagħmel hafna kummenti generici fuq ligijiet applikabbli għal kaz. Madankollu ma jghidx fejn it-Tribunal naqas fl-applikazzjoni jew in-nuqqas ta' applikazzjoni tagħhom. B'referenza għar-regolamenti kontra money laundering u finanzjar tat-terrorizmu l-Qorti tqis li dan ma hux kaz ta' hekk izda cirkostanzi fejn l-appellant mingħajr ebda intervent tas-socjeta appellata kellu komunikazzjoni ma' terz magħruf bhala 'Antrush Group Limited' sabiex fl-investiment li kien bi hsiebu jagħmel juza s-servizzi ta' transazzjonijiet digitali tal-crypto currency, cioe l-pjattaforma digitali tas-socjeta konvenuta. Ma hemm ebda hjiel jew prova li s-socjeta Foris Dax kellha xi relazzjoni f'ebda zmien ma' din il-kumpanija,

jekk tezisti. L-appellant stess ighid li skopra li dawn iffrodawh minn flusu. Mela din mhix kwistjoni ta' money laundering jew finanzjar ta' terrorizmu ghax ma ingiebet ebda prova ta' dan. L-aktar li jista' jinghad hu li l-appellant kien vittma ta' scam minn terzi. Ir-regolamenti ghalhekk mhux applikabbli ghal fattispecie tal-kaz. In kwantu ghal customer due diligence u l-implimenting procedures il-kwistjoni hawn mhix l-gharfien u l-iskrutinju tal-klijent li jirreferi ghalihom izda skrutinju tat-transazzjonijiet mat-terz li jistghu jifgħu suspett fuq il-klijent tas-socjeta li qed tipprovdi s-servizz. Il-fatt li saru 25 transazzjoni f'xahar mill-appellant ma tassumix rilevanza f'dawn ic-cirkostanzi. L-appellant ma ghamel xejn suspettuz. Uza flusu kif dehrlu hu. Kellu jew ma kellux esperjenza hu dahal ghal dan in-negozju volontarjament f'tip ta' negozju relattivament gdid u riskjuz għall-ahhar, iktar u iktar meta t-transazzjoni saru ma' 'external wallets' fejn is-socjeta appellata ma ghandha kwazi ebda hjiel ta' jew skrutinju fuq ir-ricevent tal-fond. Dan sar ghax hekk ried l-appellant mhux is-socjeta appellata. Hu minnu li f'xahar l-appellant ghamel mal-25 transazzjoni ammontanti b'kollox ghal USD200,000 imma dan ma jfissirx li s-socjeta appellata kellha xi obbligu tinforma l-appellant li qed jinnegozja wisq flus f'qasir zmien. Kif inghad l-appellant kien liberu x'jagħmel bi flusu u jekk ried jidhol ghal dan it-tip ta' negozju avolja principjant, seta' talab pariri ta' professjonisti ta' fiducja jew ma jkunx daqshekk hafif biex juza daqshekk kapital f'tant qasir zmien. Is-socjeta appellata mhix il-konsulent tal-appellant izda provveditur ta' servizz li l-appellant ghazel li juza kif dirett minn terz li l-appellant ighid li kien frodist. In kwantu għall-allegat nuqqas tas-socjeta appellata li taghti informazzjoni dwar dak li sehh biex jigu rintracciati t-terzi paragrafu 13 tar-risposta tal-appell taghti risposta li din il-Qorti bhat-Tribunal taccetta bhala verosimili.

Illi Custodial wallets huma dawk provduti minn centralised crypto exchanges bhall-appellata (fost ohrajn) tramite l-applikazzjoni digitali crypto.com. Il-klijenti jabbonaw għall-applikazzjoni u jifgħu custodial wallet fuq il-pjattaforma tal-iskambju tal-appellata li min-naha tagħhom jipprovdu lill-utenti dik li tissejjah "digital key" li huwa kodici uniku ghal kull transazzjoni jew trasferiment. Ghalhekk, sakemm it-trasferimenti magħmula minn utenti tal-pjattaforma, Cioe klijent ta' Foris Dax, huwa minn custodial wallet tal-klijent ghal custodial wallet iehor miimum minn provditur tal-istess servizz fuq pjattaform digitali ohra, l-ittraccar tat-trasferiment, flimkien ma' certu informazzjoni bhal l-identita tar-ricevitur huwa possibbli. Dan mhuwiex il-kaz fir-rigward dawk li jissejhu non-custodial wallets jew external wallets, fejn ma hemm ebda skambju fuq pjattaforma provdut minn provditur li jigbor l-informazzjoni tal-utent fl-istadju tal-abbonament, izda l-external wallet huwa mizmum direttament minghajr ebda involviment ta' pjattaforma ta' entita licenzjata. B'hekk l-identifikazzjoni tad-detentur tal- external wallet mhuwiex possibbli billi dak li jintuza huwa biss numru tal-external wallet mizmum fuq il-blockchain. Fil-kaz ta' wallets ta' dan it-tip, is-socjeta appellata ma jkollha ebda informazzjoni peress illi l-fondi li jkun intbagħtu ma jistghux jigu jintracciati;

Ghalhekk l-aggravju hu michud.

It-tieni aggravju

Dan l-aggravju jiffoka fuq kif l-appellant naqas li jiggestixxi sew l-ilment tal-appellant. Jghid li skont il-Virtual Financial Assets Handbook is-socjeta appellata naqset li tigbor l-informazzjoni kollha rilevanti biex tinvestiga l-kaz. Jirriferi ghal emails mibghuta fis-27 ta' Dicembru 2022 u 29 ta' Marzu 2023 mis-socjeta appellata lill-appellant fis-sens li jekk is-socjeta tircevi talba ufficjali mill-awtoritajiet Izraeljani tista' tikkopera magghom. Madankollu jidher minn emails esibiti illi l-awtoritajiet kienu talbu l-informazzjoni izda kienu ghadhom qed jistennew risposta. Waqt il-proceduri quddiem l-arbitru s-socjeta appellata tat ir-raguni ghaliex ma kinitx qed tikkopera mal-awtoritajiet Izraeljani. L-appellant isostni li dan id-dewmien kollu ghal ispjegazzjoni, naqqas iz-zmien biex l-appellant jiehu mizuri protettivi, issir investigazzjoni ta' x'sehh u rintraccar tat-transazzjonijiet. B'zieda ma' dan l-istess socjeta appellata ma imblokkatx il-kontijiet tal-iscammers meta sar l-ilment mill-appellant.

Jirrizulta lill-Qorti illi n-National Cyber Center tal-Pulizija Izraeljana ikkuntattjat lill-ufficju legali tas-socjeta appellata fis-27 ta' Frar 2023 fejn talbet informazzjoni fuq l-ilment tal-appellant li hu cittadin Izraeljan. B'risposta s-socjeta appellata infurmathom li hi kumpanija Maltija u kellha l-obbligi regulatorji dwar kif tinghata access ghal data personali f'sitwazzjoni transkonfinanti skont il-GDPR. Ghalhekk il-pulizija Izraeljana intalbet tuza l-procedura applikabbli. Ma jidhirx li l-kwistjoni marret lil hinn minn hekk. Is-socjeta appellata qatt ma intalbet ghal xi informazzjoni mill-awtoritajiet Maltin jew saret xi ordni tal-Qorti. Din il-Qorti ma tifhimx l-iskop wara dan l-aggravju billi s-socjeta appellata ma jidhirx li naqset f'xi dmir li wassal ghat-telf tal-appellant liema telf kien gia sehh qabel l-ilment. B'zieda ftit li xejn seta' jsir mis-socjeta appellata ghaliex meta sar l-ilment it-transferiment kien sar lil 'external wallet' li kif jirrizulta mill-provi ma hemm kwazi ebda mod ta' traccabilita tal-assi trasferiti billi t-trasferiment isir kwazi b'mod immedjat bejn il-klijent tas-socjeta appellata u t-terz f' 'external wallet' fejn l-istess socjeta appellata anqas ikollha dettalji jew informazzjoni dwarhom ghax mhux klijenti taghha.

Ghalhekk l-aggravju hu michud.

It-tielet u r-raba' aggravji

L-appellant ighid fit-tielet aggravju li r-regolamenti dwar il-Virtual Financial Assets (L.S. 590/01) ighidu li s-socjeta appellata obbligata tassigura li jkollha arrangamenti adegwati ghal protezzjoni tal-assi tal-klijenti taht il-kontroll taghha, biex igi minimizzat t-tnaqqis tal-assi rizultat ta' uzu hazin tal-assi, frodi, amministrazzjoni dghajfa fost l-ohrajn. L-appellant isostni li s-socjeta appellata ma urietx x'arrangamenti kellha u ghalkemm kellha l-obbligu li izzomm kont tat-transazzjonijiet naqset li tinforma l-awtoritajiet bi transazzjonijiet suspettuzi. Li kieku s-socjeta appellata aderiet mal-obbligi t-telf tal-appellant kien ikun anqas.

Fir-raba' aggravju tghid li s-socjeta appellata naqset fl-obbligi fiducjarji skont il-Kodici Civili billi ma wettqitx l-obbligi b'buona fede, l-onesta u diligenza. Ghandha l-obbligu li tikkumpensa lill-appellant ghat-telf ghaliex bhala s-socjeta li kellha l-kontroll tal-assi tal-appellant trid taghmel tajjeb ghat-telf li jigri bi frodi taghha, negligenza u nuqqas ingustifikat li tadempixxi mal-obbligi taghha skont il-ftehim mal-klijent u tal-licenzja. L-appellant isostni li dan in-nuqqas hu rifless fin-nuqqas tas-socjeta appellata li tiehu kont f'waqtu tan-numru konsiderevoli ta' transazzjonijiet li sehhew fi zmien qasir. Jghid li s-socjeta appellata naqset li tissorvelja transazzjonijiet li whud minnhom gew ricevuti minn klijenti ohra tas-socjeta appellata.

Il-Qorti ma taqbilx mal-appellant. L-obbligi fiducjarji tas-socjeta appellanti skont il-Kap. 16 tal-Ligijiet ta' Malta hija soggetta ghalihom safejn applikabbli. F'dan il-kaz l-appellant ghalkemm uza s-servizzi tas-socjeta appellata ghat-trasferiment tal-crypto currency tramite l-website taghha madankollu hu kien fil-pussess u kontroll shih ta' custodial wallet fejn kellu l-assi tieghu gestiti minnu f'dak imsejjah 'custodial wallet' u mhux mis-socjeta appellata. L-obbligu tas-socjeta appellata hu biss il-verifika li t-transazzjoni qed issir mill-klijent bl-obbligu li t-trasferiment mitlub mill-klijent isir bl-aktar mod hafif u efficjenti. Ir-ricevitur kien l-hekk imsejjah 'external wallet' li fuqu s-socjeta appellata ma jkollha ebda konnessjoni mieghu billi mhux maghruf lilha. L-informazzjoni li jkollha s-socjeta bhal dik appellata ghal external wallets hi limitata hafna u

ghalhekk hemm lok ghal abbuz li jrid jifhmu l-klijent ghax hu jkun ghamel il-kuntatt mat-terz u rabat ir-relazzjoni negozjali mieghu. Tant hu hekk li mhux kontradett li s-socjeta appellata ma tipprovdix 'external wallets' bhala parti mis-servizzi taghha. Ghalhekk mhux bizzzejjed ghall-appellant li jiccita obbligi naxxenti minn legislazzjoni sussidjarja jew il-Kapitolu 16 minghajr ma jorbot in-nuqqas allegat mal-fattispecie tal-kaz. L-appellant jorbot in-nuqqasijiet allegati ma' fatt ossia t-trasferimenti minnu maghmulin lil terz allegatament frodist. Inness tas-socjeta appellata hu biss il-fatt li l-appellant uza bi ftehim s-sistema digitali taghha biex ikollu mezz (custodial wallet) kontrollat u utilzzat minnu biss biex jaghmel negozju ma' terzi li f'dan il-kaz lanqas kienu 'custodial wallets' provduti mis-socjeta appellata. L-ghazla ta' dan il-modus operandi kien tal-appellant li messu kien jaf ir-riskji u l-incertezzi li jipprovdidi dan is-suq. Minflok ghazel jidhol ghar-riskju u fi zmien ferm qasir ittrasferixxa volontarjament somma konsiderevoli lil terzi li magghom is-socjeta appellata ma kellha ebda relazzjoni. L-arbitru fil-fatt ighid

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.

In summary, it seems conceivable that the Complainant has been the victim of an alleged scam. Whilst we fully empathize with Mr Cohen in this regard, it cannot be overlooked that he had willingly, according to his statements, transferred his virtual asset holdings from his Crypto.com Wallet to external wallet addresses which he has no access to.

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 or the veracity of any third-party or (or the instructions received from the Complainant themselves.)' [p. 123-124]

The Complainant made a transfer of his digital assets (USDT) using the Crypto.com app. The said transfers were made to three different external wallet address allegedly used by fraudsters. The transfers were made on the specific instructions of the Complainant. External wallets are recognised only by their number and their proprietors or beneficial owners are not known to the transferor. The Service Provider has no obligation under current regulatory regime to keep or make available information relating to external wallets.

The Arbitrator 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 lfs 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.

Furthermore, the Complainant must have himself 'whitelisted' the address giving all clear signal for the transfer to be executed. In fact, the Complainant himself did not raise any suspicion or evidence that there was any link between the Service Provider and the external wallet address he himself provided.

The Complainant seems to have only contacted the Service Provider after all alleged fraudulent transactions were executed.

Ma jridx wiehed jinsa l-kundizzjoni 7.2 tal-ftehim li bih l-appellant accetta s-servizz tas-socjeta appellata.

L-abritru fil-fatt ighid:

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. Whilst we fully empathize with Mr Cohen in this regard, it cannot be overlooked that he had willingly, according to his statements, transferred his virtual asset holdings from his Crypto.com Wallet to external wallet addresses which he has no access to.

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 or the veracity of any third-party or (or the instructions received from the Complainant themselves.' [p. 123-124]

The Complainant made a transfer of his digital assets (USDT) using the Crypto.com app. The said transfers were made to three different external wallet address allegedly used by fraudsters. The transfers were made on the specific instructions of the Complainant. External wallets are recognised only by their number and their proprietors or beneficial owners are not known to the transferor. The Service Provider has no obligation under current regulatory regime to keep or make available information relating to external wallets.

The Arbitrator 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 lfs 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.

Furthermore, the Complainant must have himself 'whitelisted' the address giving all clear signal for the transfer to be executed. In fact, the Complainant himself did not raise any suspicion or evidence that there was any link between the Service Provider and the external wallet address he himself provided.

The Complainant seems to have only contacted the Service Provider after all alleged fraudulent transactions were executed.

Decide

Ghal ghal dawn ir-ragunijiet l-Qorti qed taqta' u tiddeciedi billi tichad l-appell ta' Janiv Cohen, bl-ispejjez kontrih.

Mark Chetcuti

Prim Imhallef

Anne Xuereb

Deputat Registratur