Before the Arbiter for Financial Services

Case ASF 069/2024

UP

('the Complainant')

vs

Foris DAX MT Limited (C 88392)

('Foris DAX' or 'the Service Provider')

Sitting of 5 September 2024

The Arbiter,

Having seen **the Complaint** dated 15 April 2024[1] relating to the Service Provider's alleged failure to prevent, stop or reverse the payment in crypto of USDT 76,304.96[2] made by the Complainant himself from his account held with *Crypto.com* to an external wallet allegedly owned by third parties who could be fraudsters or connected to fraudsters.

The Complaint

The Complainant opened an account with the Service Provider on 24 March 2023. Between 04 April 2023 and 16 May 2023, he carried out 5 transactions involving transfer of fiat currency amounting to Euro 72,350. On each of the five occasions, the funds were immediately converted to USDT and transferred out to the said external wallet.

[1] P. 1 - 6 and attachments p. 7 - 52

[2] Tether (USDT) is a stable coin pegged at 1-to-1 with a matching fiat currency and backed 100% by Tether's reserves.

The fiat currency transfers seem to have originated from a financial institution named OpenPayd.

The Complainant stated that:

'*In March 2023, I was presented with an investment opportunity that ultimately resulted in a significant financial loss. I was initially contacted online by an individual who claimed to be investing through the platform 'tethererc20.info'. This, as it turned out, was a Smart Contract, and upon the simple act of clicking a button, malicious actors were able to gain unauthorized access to the designated wallet, subsequently extracting the funds within. While I did not initiate direct payments, I transferred funds from my Crypto.com wallet to my TrustWallet, which happened to be connected to the fraudulent platform. Consequently, the perpetrators were able to successfully siphon all the USDT I had deposited. An in-depth analysis of the blockchain activity subsequently revealed that my TrustWallet address had been flagged due to its association with illicit activities. This association arose from the presence of malware that had compromised my wallet, leading to the fraudulent extraction of my assets. Therefore, it is not clear how the transactions that I was directing towards my TrustWallet from Crypto.com were not flagged by the crypto exchange. It is important to note that Crypto.com, as a regulated financial entity, possesses the necessary tools to identify and mitigate such financial crimes, thus preventing victimization by either blocking suspicious transactions or subjecting them to rigorous scrutiny. However, these safeguarding mechanisms were not adequately deployed, which raises concerns regarding Crypto.com's adherence to Anti-Money Laundering (AML) and Know Your Customer (KYC) regulations*.'[3]

Complainant basically raises these issues:

- Service Provider should have realised that external wallet to which the USDT were being transferred was owned by fraudsters operation as TrustWallet on a platform 'tethererc20.info'.
- Crypto.com should effectively communicate the potential risks associated with non-custodial wallets to their users and implement appropriate

[3] P.3

measures when they observe significant transactions being directed to non-custodial wallets from their platforms.[4]

- The wallet address to which Complainant claims to have sent his funds for several times, corresponding to his cold wallet hosted by TrustWallet, was flagged by the tracing software because its movements were associated with a fraudulent scheme, since the fraudsters gained access to his wallet via a Smart Contract, and they started to conduct activities without his consent.[5] [6]

The Complainant accused the Service Provider of misconduct, neglect, misrepresentation, violation of international law, and lack of vigilance and, therefore, expects full remedy for his losses of USDT 76,306.94.

Reply of Service Provider[7]

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'**) and the purchase and sale of digital assets through the Wallet. Services are offered through the Crypto.com App (the '**App'**). The Wallet is only accessible through the App and the latter is only accessible via a mobile device.*

- *Our company additionally offers a single-purpose wallet (the '**Fiat Wallet'**), which allows customers to top up and withdraw fiat currencies from and to their personal bank account(s) for the purposes of investing in crypto assets. This service is offered by the legal entity Foris MT Limited.*

[4] P. 7
[5] P. 18
[6] In his evidence (p. 74) Complainant confirmed that all transfers from his wallet at Crypto.com to TrustWallet were performed with his authority, so here he is probably referring to movements out of the unhosted TrustWallet.
[7] P. 58 - 65 and attachments p. 66 - 72

- *Mr UP (the '**Complainant**'), e-mail address XXX.YYYYYY@live.it, became a customer of Foris DAX MT Limited through the Crypto.com App and was approved to use the Wallet on the 24th of March 2023.*
- *The Company notes that in the submitted complaints file, Mr UP's representative has outlined his desired remedy as: (i) reimbursement for incurred financial losses.'*[8]

They gave a detailed sequence of the various transactions executed by the Complainant on his wallet.[9]

They concluded that:

'*In summary, Mr UP has withdrawn the total amount of 76,306.94 USDT (approximately 71,663.59 EUR based on market conditions as of April 19, 2024) from his Crypto.com Wallet towards an external wallet address between April 5, 2023 – May 16, 2023.*

The wallet address in question is:

0x40508Bb34f92d972535022bA814ceDdf908845b3

Based on our investigation, the Company has concluded that we are unable to honour the Complainant's refund request based on the fact that the reported transfers were made by Mr UP himself.

While we sympathize with the Complainant and recognize that he may have been misled or induced into transferring funds to an alleged fraudster, it is important to note that these transfers were made solely at the Complainant's request. We must also emphasize that the address the funds were transferred to does not belong to the Company and as such, any due diligence of the ownership of this address falls under the responsibilities of the provider of said wallet.

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

[8] P. 58
[9] P. 59 - 64

Mr UP 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 UP in this regard, it cannot be overlooked that he had willingly, according to the statements in the received complaint letter, completed the transfers in question.

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.'[10]

Hearings

During the first hearing held on 10 June 2024, the Complainant said:

'*Last year, I have made five money deposits from Crypto.com website to my personal Wallet.*

Sometime after I sent this money, I understood that my money was stolen from my Wallet.

To clarify, after I deposited the money in my Wallet, they were joined with another external website which at the beginning did not seem like a scam website.

After three months, I understood that the website which held my Wallet had an alert that it was a potential scam website. I reported the fraud and only later was this website proved to be a fraud.

When I sent my money from my Wallet, the amount of money was really big. I feel that there was a lack of control by Crypto.com because the amount of money was strange in that account and it was divided in five transactions in my Wallet. Crypto.com should have had more control of this account.'[11]

On being cross-examined, he said:

'Asked whether I deposited Euros into my Crypto.com account and then purchased cryptocurrency with this money and then transferred it from my Crypto.com Wallet to another Wallet account, I say yes.

Asked with what website was this personal Wallet opened to which I transferred this cryptocurrency, I say that it was TrustWallet.

Asked whether TrustWallet is the Wallet belonging to the website which eventually I discovered was a scam website, I say that, yes, it was the same Wallet.

[10] P. 64 - 65
[11] P. 73

I confirm that I personally withdrew funds from my Crypto.com account and sent them to my Trust Wallet address and that Crypto.com followed my instructions in transferring the funds from my Crypto.com account to the TrustWallet account.

Asked from where I obtained this TrustWallet address, I say from the App TrustWallet.

***Mr UP would like to add this to his testimony**:*

I transferred money from the bank to Crypto.com and from there I sent the money to TrustWallet.

I feel that Crypto.com has all the tools to analyse the address of my Wallet. I understand that a simple research would have proved that my Wallet was linked to a scam website.

I say that at the beginning, there was no sign of a scam.[12]

During the second hearing on 15 July 2024, the Service Provider strongly denied that during the period when payments were being processed with full authority of the Complainant, they had any information which could have raised suspicions on the fraudulent nature of the recipient wallet which was external and not hosted by Crypto.com.

They affirmed that the information that emerged later about the fraudulent nature of the recipient wallet was irrelevant to this Complaint as payments on blockchain cannot be reversed.

Final Submissions

In their final submissions, the parties largely restated their arguments made in the Complaint, the Reply and the hearings.

The Complainant concluded that:

'*The following points of negligence emerged in this case:*

[12] P. 74

1. *Absence of Risk Assessment: there was no evidence of a thorough risk assessment conducted on my financial activities, leaving me vulnerable to potential financial harm.*

2. *Lack of Transaction Monitoring: despite engaging in transactions with significant volumes and exhibiting unusual financial activities, Crypto.com failed to detect suspicious patterns or anomalies, as required by regulatory standards.*

This can also be found in specific points outlined in Crypto.com Terms of Agreement particularly sections 12.7 and 24.20(f), which emphasize their obligation to monitor accounts and transactions for compliance with applicable laws, including those related to anti-money laundering (AML) and counter-terrorism financing (CTF).

While it is indeed true that I was authorizing the transactions from my Crypto.com wallet to the other wallet, which was my DeFi wallet from where the scammers took all the funds via a smart contract – namely me clicking on a link which gained them access to the funds – it must also be noted that, via the blockchain analytics tools available to Crypto.com, it was clear that the wallet where I was directing the funds from Crypto.com wallet was marked as associated with flagged activities. This is because it was linked, as outlined above, to an address as CDA blacklisted as it was involved in a huge scam network.'[13]

The Service Provider submitted:

'***<u>Issue (1) – Gross Negligence</u>***

4. *As demonstrated in the Respondent's Reply to the Complaint, between 5 April to 16 May 2023, over the course of five transactions, the Complainant sent a total of 76,306.94 USDT from his Account to the same external cryptocurrency wallet (the '**External Wallet'**). These withdrawals, the Disputed Transactions, were successfully executed in accordance with the Complainant's express instructions.*

[13] P. 79

5. *On the basis of the Complainant's oral testimony given at the first hearing on 15 July 2024, and his Final Summary dated 30 July 2024, the Complainant alleges that he fell victim to a scam. The Complainant admitted to opening an account with the Respondent and to making the Disputed Transactions.*

6. *The Respondent is naturally only in possession of information relating to and provided by its customers. It is highlighted that the External Wallet is not one which the Respondent provides services to, and as such, is not a wallet that the Respondent has any user/client information on. In fact, the Complainant has given oral evidence to the fact that the External Wallet is his own decentralized wallet supported by TrustWallet. For the Tribunal's context, TrustWallet is likely a reference to a non-custodial wallet offered by Trust, the brand name of DApps Platform, Inc. A non-custodial wallet is one where the user themselves have control over the private keys which allow one to access the wallet. In his own testimony, the Complainant has suggested that the Material Transactions are simple withdrawals of cryptocurrency from the account he held with the Respondent to another non-custodial account held by himself. TrustWallet has no connection or affiliation to the Respondent.*

7. *The Respondent has no connection with tethererc20.info, the alleged fraudsters or TrustWallet.*

8. *As outlined in document FS-1, the Complainant is solely responsible for the security and authenticity of all instructions submitted through the App. As set out in Clause 7.2(b) & (d) of the Terms and Conditions, the Respondent does not play any role in second guessing the purpose of customer transactions and a simple withdrawal of cryptocurrency would not raise any alarms, particularly when withdrawal addresses are whitelisted by users prior to being eligible for a withdrawal. Once sent, a transaction occurring on the blockchain is designed to be immutable and irreversible.*

9. *It is also important to note that the Complainant claims to have sent the Disputed Transactions to the External Wallet which belongs to himself and that the scammers had gained unauthorized access to the External Wallet due to his negligence by way of clicking on a link.*

10. *On the balance of the foregoing, while the Complainant seems to have fallen victim to a scam, it is the Respondent's case that the Complainant should be responsible for any losses which occurred out of his own gross negligence.*

11. *In summary, the Respondent would submit that the Disputed Transactions were authorized by the Complainant and the Respondent ultimately bears no responsibility for merely carrying out the Disputed Transactions as instructed through the Complainant's Crypto.com App account*.

Issue (2): Risk Assessment and Transaction Monitoring

12. *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.*

13. *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.*

14. *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 share details of the internal monitoring results for any individual cases.*

15. *Nonetheless, it is respectfully submitted that the Arbiter is not competent authority to adjudicate or hear allegations relating to AML and CTF matters as these should be dealt with by the FIAU in accordance with Chapter 272 of the Laws of Malta.*

16. *The Respondent would also like to emphasize that any alleged subsequent flagging of wallets as being associated with illicit activities usually occurs after the illicit activities have occurred and been reported. No evidence has been provided to show that the External Wallet belonging to the*

Complainant himself, had been flagged at the material time the Disputed Transactions occurred.'[14]

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

Further Considers:

The Merits of the Case

The Arbiter is considering the Complaint and all pleas raised by the Service Provider relating to the merits of the case together to avoid repetition and to expedite the decision as he is obliged to do in terms of Chapter 555[15] which stipulates that he should deal with complaints in '*an economical and expeditious manner*'.

The Service Provider

Foris DAX is licensed by the Malta Financial Services Authority ('MFSA') as a VFA Service Provider as per the MFSA's Financial Services Register.[16] It holds a Class 3 VFAA licence granted on 16 April 2021, by the MFSA pursuant to Article 15 of the Virtual Financial Assets Act, 2018 ('VFAA').

As per the unofficial extract of its licence posted on the MFSA's website, the Class 3 VFAA Licence authorises Foris DAX to provide the following VFA Services: (i) Execution of orders on behalf of other persons (ii) Dealing on own account and (iii) Custodian or Nominee Services to Experienced and Non-Experienced investors.[17]

As outlined in the disclaimer section of the *Crypto.com* website, Foris DAX is *'trading under the name 'Crypto.com' via the Crypto.com app'*. [18]

[14] P. 83 - 85
[15] Art. 19(3)(d)
[16] https://www.mfsa.mt/financial-services-register/
[17] https://www.mfsa.mt/financial-services-register/
[18] https://crypto.com/eea/about

The Application

The *Crypto.com App* is a mobile application software developed, owned and released by Crypto.com and available for download for Android or Apple iOS.

It offers the account holder *'a crypto custodial wallet'* and *'the purchase and sale of digital assets on own account'*.[19]

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 an external wallet address admittedly belonging to the Complainant but allegedly penetrated and used by fraudsters. The transfers to the external wallet 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.

[19] P. 83

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'*[20] 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[21] also issued Implementing Procedures on the Application of Anti-Money Laundering and Countering the Funding of Terrorism Obligations to the Virtual Financial Assets Sector.[22] 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

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

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 EUR 72,000.

  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 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 obligation for VFAs to identify the beneficial owners of unhosted wallets was not part of the regulatory regime at the time of events that gave rise to this Complaint. VFAs obligations of due diligence relate to their own customers, in this case, the Complainant, not to owners of the unhosted wallets recipients of crypto assets transferred by their client.

  Obligations for VFA's to identify such beneficiaries will only enter into force in 2025 in terms of **EU REGULATION 2023/1113 of 31 May 2023 on information accompanying transfer of funds and certain crypto assets** as further explained in the **EBA Guidelines on information requirements in relation to transfers of funds and certain crypto-assets transfer under**

Regulation EU 2023/1113 (Travel Rule Guidelines – reference EBA/GL/2024/11 of 04/07/2024).[23]

- 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'* owned by the Complainant and, hence, the Service Provider had no information about the third party to whom the Complainant was actually transferring his crypto assets.

  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 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).[24]

  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

[23] In particular article 4.8 para 76 - 90

[24] E.G. https://www.chargebackgurus.com/blog/chargebacks-more-volatile-complex-than-cryptocurrency

Instructions for a Digital Asset Transfer to Crypto.com as the Digital Asset Transfer may not be cancelled or reversed once processed …'.[25]

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:[26]

'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 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.

The current 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.[27]

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 financial institution that made the fiat currency transfers to his Crypto account.

[25] P. 99
[26] *Ibid*.
[27] Financial institutions based in Malta are regulated under a separate and distinct regulatory framework, namely, that provided for under 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).

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 is in any way related to the Service Provider.

- Ultimately, the Arbiter does not consider that in the case in question, there is any clear and satisfactory evidence that has been brought forward, and/or emerged, during the proceedings of the case which could adequately corroborate that the Service Provider failed in any of the applicable obligations, contractually and/or arising from the VFA regulatory regime applicable in respect of its business.

- The Arbiter notes that the crypto business is a relatively new area with no *harmonised regulation* existing at the time of the disputed transactions.

  A regulatory framework is still yet to be implemented for the first time in this field within the EU.[28]

  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.[29]

[28] 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/

[29] https://www.eiopa.europa.eu/document-library/other-documents/crypto-assets-esas-remind-consumers-about-risks_en

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.[30]

The Arbiter notes the strong denial of the Service Provider that at the time when the transfers complained of were taking place they had any indication in their monitoring system that the address of the unhosted wallet was in any way connected to a fraudulent activity.

Furthermore, whilst the Complainant claimed that he found evidence that this TrustWallet was connected to fraudsters, he did not provide any evidence that there was any such information in the public domain that the Service Provider should have spotted at the time these transfers were taking place.

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.

https://www.esma.europa.eu/sites/default/files/library/esa_2022_15_joint_esas_warning_on_crypto-assets.pdf

[30] P. 84

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.[31]

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

Alfred Mifsud
Arbiter for Financial Services

[31] 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.