Before the Arbiter for Financial Services

Case ASF 137/2022

NW ('the Complainant')

vs

Foris DAX MT Limited (C 88392)

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

Sitting of 12 December 2023

The Arbiter,

Having seen the **Complaint** dated 21 November 2022[1] relating to a loss of €15,000 suffered by the Complainant as a result of transfer of such an amount on 14.07.2021 to Transactive Systems UAB in an IBAN account based in Lithuania in the name of Foris DAX MT.

The Complaint

The Complainant maintains that:

> *"he never made on his own a transaction order of any part of the crypto allegedly credited to his Crypto.com wallet in consideration of the payment of the EUR 15,000".*[2]

In his Complaint, the Complainant lists various information he has requested from the Service Provider to enable him to understand how the funds transferred were

[1] P. 1 - 38
[2] P. 3

converted to Bitcoin (BTC) but that soon afterwards these disappeared from his Crytom.com account. He complains that:

> *"Foris Dax MT received an amount of EUR 15,000 from the Complainant but fails to provide any proof that the goods/services for which this amount has been paid, are provided to the Complainant.*
>
> *Second, Foris Dax MT fails to provide proof that the wallet on the name of (Complainant) was not accessed by a third party in breach of privacy and security requirements of the platform.*
>
> *Third, Foris Dax MT fails to disclose information to the wallet holder (such as wallet access data, transaction record etc) which would allow the latter to protect his justified legal interest."*[3]

By way of remedy, Complainant seeks compensation from the Service Provider for €18,500 being the original €15,000 transferred from his bank account and a further €3,500 for costs associated with legal remedies used.[4]

Reply of Service Provider

The Service Provider replied on 09 December 2022 stating that:

> "*Foris DAX MT Limited (the 'Company') offers the following services: a crypto custodial wallet (the 'Wallet'), the purchase and sale of digital assets on your 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, inter alia, 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 latter is only accessible via a mobile device.*

[3] *Ibid*.
[4] *Ibid*.

> *Mr NW (the 'Complainant'), e-mail address: XXXXXXXXX@gmail.com, became a customer of Foris DAX MT Limited through the Crypto.com App and was approved to use the Wallet on 22 June 2021."*[5]

They confirmed that apart from the €15,000 funds transferred by Complainant on 15 July 2021, his Crypto.com account shows that he had earlier, on 01 July 2021, bought BTC 0.02 for the then current value of €566.32 funding from his personal debit/credit card.

The €15,000 were immediately converted into BTC 0.5477385 and then all BTC holdings were transferred to an external wallet which had been whitelisted[6] by the Complainant.

The Service provider also confirmed that all information requested by the Complainant had been provided via a secure file sent by email on 18 May 2021.[7]

The Service Provider concluded that:

> "*In regards to all of the account activity outlined earlier in the Timeline, we have observed no new unique logins from a new mobile device, and all transactions were executed using the account's unique login credentials. Our audit trail shows that no change of passcode or login credentials, or any failed login attempts, have been registered for the Complainant's Wallet hence one can conclude that the Wallet has been accessed with the same credentials used before the date of the reported incident – the same email address and passcode.*
>
> *Based on our investigation and the facts laid out above, the Company is of the opinion that we cannot honor the Complainant's refund request. The 15000 EUR deposited on 15 July 2021, has been utilized in the purchase of digital assets which have subsequently been withdrawn from Mr NW's Wallet and the Company has no reason to believe that unauthorized access took place."*[8]

[5] P. 44
[6] Whitelisting is the process by which an external wallet is approved by the account holder for withdrawals of digital assets.
[7] P. 47
[8] *Ibid*.

The hearings

The first hearing was called for 28 March 2023, but Complainant failed to join, and the hearing was postponed to 18 April 2023. For the second time, the Complainant failed to make presence.

The first proper hearing was held on 16 May 2023 where the Complainant submitted:

> "***This is a case regarding a scam of €15,000. The scammer gave me instructions.***
>
> ***Here, in Finland, I found on the social media where I could put money in crypto. and I … and then Ryan Lauren called me and explained what I must do.***
>
> ***(Asked by the Arbiter if Ryan Lauren was representing the service provider, Foris DAX, I say, yes).***
>
> ***I say that the scammer gave me instructions. This was my first time registering for crypto assets. Then, I loaned €15,000 from the banks and then I gave the order to Lauren to transfer the €15,000 into a crypto account and to convert it into a crypto asset. I tried to contact the crypto account on my phone at Lauren's request. This order was immediately successful. I got the money in my account on my phone. I say that €15,000 was transferred here from the Resurs bank account to which the money was borrowed from Resurs. The amount was visible on the account for one day and I could see it in my phone for one day and then it disappeared from there within one day, I do not know where. Someone transferred the money to somewhere, not me. I did not give the instructions for those crypto assets to be transferred to someone else. Somebody created an account for me in Lithuania bank under my name. When I tried to enquire about my account information from there, it was not accepted.***
>
> ***I say that this happened in July 2021. After this, when I could not see this in my account, when somebody transferred them to an account that I did not know about, I asked the Lithuania bank because I understood that the account was in my name but they told me nothing. I asked Crypto.com***

but they told me nothing. I do not remember the date when I asked Crypto.com but there is on my email.

My complaint is that Crypto, Foris DAX MT, transferred my crypto assets from my account without my knowledge, and I am holding them responsible and seeking recovery of my funds and legal expenses. I have never made any transfers or gave orders.

I requested information from Crypto.com but they did not give me this information."[9]

During cross-examination, the Complainant said:

"***I confirm that I was the one who uploaded the Crypto.com App on my phone and opened my account with Crypto.com.***

I confirm that I have made deposits in Euros in my Crypto.com account. Yes, I remember transferring €15,000 from my bank account to my Crypto.com account. I confirm that this was done sometime arount 15 July 2021. I say that I got the orders from Ryan Lauren; he told me to deposit €15,000 in my crypto account, nothing else.

I confirm that Ryan Lauren helped me back in July 2021 with my Crypto.com App on my telephone through Any Desk. I used to have Any Desk but not anymore.

Asked whether I understand that by using the Any Desk App, I grant him access to my telephone and he could control things, I say, yes. I was stupid.

It is correct to say that I do not remember myself making any transfers of the cryptocurrency from my App out of my Crypto.com App.

I confirm that I made the order to exchange €15,000 into Bitcoin. I saw this reflected in my Crypto.com balance for just one day. Then, it disappeared.

It is being said that in 2021, Crypto.com had provided me through a secured link the data I requested and asked whether I received this, I say

[9] P. 53 - 54

> ***that I do not remember. It is being said that a secured file was sent to my email, I say that it is possible.***
>
> ***The service provider stated that apart from the €15,000 we are talking about, on 1 July 2021, i.e, two weeks before, there was a small transfer of €566 in my account. Asked by the Arbiter whether I know anything about that transfer, if I made that transfer, I say that no, I did not make that transfer. It seems that somebody, after I opened my account, gave me a gift of €566. I did not make this***."[10]

The second hearing was held on 06 June 2023 where the Complainant appointed to represent him at the hearing Mr Boris Ivanov of Legal Services Agency of Bulgaria.

The Service Provider submitted:

> ***"The transactions complained of from Mr Makela's side relate to some purchases, transfers and withdrawals of cryptocurrency. From what we can see and from what has been submitted from the side of the complainant, purchases were firstly made on the 1 July; subsequently again on the 15 July and, finally, a withdrawal was also made on the 15 July 2021.***
>
> ***From what we can see, the transaction was performed through the same login, combination email and passwords from the same mobile device and transactions were made using the same login credentials as his sign-in device. So that is to say that, on our side, there is no evidence to show that there was any change in the login credentials that authorised the transactions.***
>
> ***From our side, we would therefore say that these transactions were authorised by the complainant himself. On the basis of that, there is no reason why the service provider should be responsible for any of the withdrawals made given that these were instructions received from the complainant himself.***

[10] P. 54 - 55

> ***What transpired in the evidence of the complainant is that he allegedly gave someone by the name of Ryan Lauren access to his phone or to his device and allegedly this Ryan Lauren performed these transactions through an App called Any Desk which allows someone from a remote destination to control the device in question so long as the person who owns the device gives this third party access to it. There is no way we can confirm this – it is the evidence of the complainant himself. But what we would say is that if he indeed gave access and secure access of his device, and his passwords and credentials to a third party to perform these transactions, then he is also responsible for these transactions because of the way he gave access to his device. This is covered in the Terms and Conditions which we have filed with the OAFS (FS-1).***
>
> ***Apart from that, we have to say that we have no affiliation to this Ryan Lauren. From the evidence of the complainant, he is the one who sought Ryan Lauren's help; he is the one who permitted Ryan Lauren to convince him to download this Any Desk device App. We also have no relation to this Cryptomatix.com website which is alleged in the papers filed to the OAFS by the complainant.***
>
> ***On the balance of the foregoing and on the whole, we would say that we are not responsible for these transactions or what transpired after these transactions. We simply carried out the transactions as instructed by the complainant. And, in the event that the complainant willingly gave access of his secured device, his secured lock and credentials to a third party who then performed these withdrawal actions, it is for the complainant himself to be responsible for anything that happens as a consequence of his own actions."***[11]

Mr Boris Ivanov requested an opportunity to make further submissions on behalf of the Complainant as he was not given opportunity to assist the Complainant in the hearing of 16 May 2023. The Arbiter exceptionally made a concession and invited Mr Ivanov to make additional submissions which were received on 30 August 2023.[12]

[11] P. 87 - 88
[12] P. 90 - 96

In these submissions, the Complainant made a case that the Service Provider claims in their publicity that they have the tools to comply with FATF Travel Rule but effectively could not produce the evidence on the beneficiary of the wallet that the digital assets were transferred to as required under the said Travel Rule.

> "***Based upon the above, we see a clear relation between the failure of Crypto.com to comply with the FATF standards as they self-proclaimed on their website and the impossibility of the Complainant to receive partial or full recovery of his losses from the persons actively taking part in the fraudulent scheme. In this way, Crypto.com conclusively contributed to the occurrence of the Complainant's losses and his inability to seek for recovery in an appropriate manner***."[13]
>
> "***In consideration of the misleading information about Crypto.com being FATF compliant, if Crypto.com fails to provide the required information under the FATF travel rule, Crypto.com should be held liable for compensation to the complainant because such failure hinders the recovery options for the complainant.***"[14]

The Service Provider replied to the fresh submissions of Complainant on 15 September 2023 stating:

> ***"FATF Guidelines***
>
> 10. ***In the first instance, the FATF Guidelines are simply not applicable. Aside from being merely guidelines and not law, neither is the rule cited by the Complainant applicable to the factual matrix of this case.***
>
> 11. ***It is respectfully submitted that the Complainant has misconstrued the purport of the travel rule and the FATF Guidelines in respect of the Respondent's obligations and responsibilities.***
>
> 12. ***The purpose of the FATF Guidelines is directed at jurisdictions and not individual service providers, as recommendations to***

[13] P. 95
[14] P. 96

countries to include these measures in domestic legislation. Moreover, the guidelines are not law.

13. ***In fact, they are referred to as 'recommendations'. They have not been implemented into domestic law, neither by way of EU directly applicable regulations. For example, the revised Wire Transfer Regulation (WTR II) do not apply until December 2024.***

14. ***In addition, the purpose of the guidelines is to provide recommendations with the purposes of combating money laundering (AML) and the financing of terrorism (CFT) and NOT to detect fraud which has been committed as in this Complaint. If at all, this would be a regulatory matter and for the regulatory authority (FIAU) to audit the company for the purposes of assessing the measures put in place to combat AML and CFT.***

15. ***On the merits, but without prejudice to the above, footnote 30 on page 39 of the FATF: Updated guidance for a Risk-Based Approach (the 'Guidelines'), highlights that 'To date, the FATF is not aware of any technically proven means of identifying the VASP that manages the beneficiary wallet exhaustively, precisely, and accurately in all circumstances and from the VA address alone'. Therefore, in view of the nature of the industry, it is recognised that identifying the third- party wallet is not always possible.***

16. ***Moreover, again on the merits and without prejudice to the above, given that the third-party wallet was an unhosted wallet, in terms of the Guidelines on page 51 (FN 39) 'To date, FATF is not aware of any technically proven means*** **of identifying the person that manages or owns an unhosted wallet** ***precisely and accurately in all circumstances. Countries should be aware of this and also note that the result of the analysis using such tools should be considered as reference information only.'***

Allegations of Misleading Information

17. ***In this respect, the Complainant's submissions of Crypto.com providing any misleading information are strongly and strictly refuted, and it is submitted that these allegations are carelessly raised by the Complainant. Neither has the Complainant proven that such information was misleading. The Complainant is invited not to misguide the Arbiter for Financial Services.***

CIMA Industry Notice

18. ***This can be dealt with swiftly. The Complainant has simply conflated the Crypto.com Exchange with the Crypto.com App. The Crypto.com Exchange is a separate product provided by the Crypto.com Group, and more particularly, by a regulated, licensed entity in the Cayman Islands. To the extent that any materials regarding the Crypto.com Exchange are concerned, they do not apply to the Crypto.com App.***

19. ***In any case, it can be seen from the Complaint's own screenshot that the relevant regulations did not come into effect until 1 July 2022. The disputed transactions predate this date by quite some time, dating from 1 July 2021 – 15 July 2021. Even if these regulations were relevant or applied to the Crypto.com App (which is denied), these regulations simply do not have any relevance to the current facts."***[15]

During a further hearing held on 19 September 2023, the parties agreed to proceed with final written submissions.

Final Submissions

No new information emerged from the final written submissions wherein both parties re-stated their earlier explained positions, with Service Provider re-asserting that they have no connection with the alleged fraudsters.

[15] P. 101 -102

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[16] 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.[17] 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.[18]

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'*. [19]

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...'*.[20]

It offers the account holder *'a crypto custodial wallet'* and *'the purchase and sale of digital assets on own account'*.[21]

[16] Art. 19(3)(d)
[17] https://www.mfsa.mt/financial-services-register/
[18] https://www.mfsa.mt/financial-services-register/
[19] https://crypto.com/eea/about
[20] P. 60
[21] P. 44

Observations & Conclusion

Summary of main aspects

The Complainant has admitted that he was scammed by fraudsters to whom he gave access to his Crypto.com App through Any Desk software. In so doing, he gave the fraudsters full access to his credentials which falls clearly in the category of gross negligence. In fact, in the hearing of 16 May 2023 he stated: ***"I was stupid".***[22]

In essence, the Complainant is seeking compensation from Foris DAX for the Service Provider's alleged failure to prevent, stop or reverse the payment he made to an unknown external wallet presumably under control of the fraudster, particularly for failing to implement the recommendations of FATF Rule 16 Travel Rule which they claim obliges the Service Provider to keep records on the identity of the holders of the recipient external wallet.

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.

Furthermore, the Service Provider made a strong argument that FATF Travel Rule 16 is simply a recommendation which is not yet binding; it is related to Anti-Money Laundering issues not within the competence of the Arbiter and that claims of compliance to FATF Rules made by other members of the Crypto.com group related to other products have no relevance to this Complaint.

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').

[22] P. 54

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'*[23] 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').

FATF Travel Rule

FATF Recommendation 16 (Travel Rule)[24] was originally designed for wire transfers in the traditional financial system. In June 2019, this recommendation was extended to include VASPs but very few countries have yet passed legislation to adopt it and even fewer have begun enforcing it and supervising it. In the EU, the Markets in Crypto-assets regulation (MiCA) is expected to incorporate the crypto travel rule by January 2025.

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

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

[24] 16. Wire transfers * Countries should ensure that financial institutions include required and accurate originator information, and required beneficiary information, on wire transfers and related messages, and that the information remains with the wire transfer or related message throughout the payment chain. Countries should ensure that financial institutions monitor wire transfers for the purpose of detecting those which lack required originator and/or beneficiary information and take appropriate measures. Countries should ensure that, in the context of processing wire transfers, financial institutions take freezing action and should prohibit conducting transactions with designated persons and entities, as per the obligations set out in the relevant United Nations Security Council resolutions, such as resolution 1267 (1999) and its successor resolutions, and resolution 1373(2001), relating to the prevention and suppression of terrorism and terrorist financing.

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.

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 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 himself had 'whitelisted' the address giving all clear signal for the transfer to be executed**.**

  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 …'.[25]

[25] P. 72

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'.

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 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.**

  Furthermore, if the Complaint and the claim for compensation are based on Anti-Money Laundering and Financing of Terrorism, the Arbiter has no competence in AML/FT issues and such matters should be referred to the competent authority (FIAU MALTA).

[26] P. 73

However, the Arbiter is confident that a single payment of €15,000 does not give rise to any issues regarding the FIAU's Application of Anti-Money Laundering and Countering the Funding of Terrorism Obligations of the Virtual Financial Assets Sector – Implement Procedures PART 2.[27]

- 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]

[27] FIAU Part II (fiaumalta.org)

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

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 in this sector.

In fact, the Arbiter notes that apart from the fraud aspect of this loss, Complainant bought into BTC at quite peak prices and, fraud apart, he would still be nursing considerable investment losses.

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.[30]

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

Alfred Mifsud
Arbiter for Financial Services

[30] 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.