

Before the Arbiter for Financial Services

Case ASF 158/2021

AG

(‘the Complainant’)

vs

Foris DAX MT Limited

**(C88392) (‘Foris DAX’ or ‘the Service
Provider’)**

Sitting of the 5 December 2022

The Arbiter,

Having seen **the Complaint** relating to the Service Provider’s alleged failure to prevent, stop or reverse the payment in crypto (Ethereum) made by the Complainant from his account held with *Crypto.com* to a third party who was allegedly a fraudster.

The Complaint

The Complainant explained that he has been scammed by a fraudulent trading company utilizing the services of *Crypto.com*.

He noted that he never willingly created an account, nor has he confirmed the transactions. The Complainant explained that it was all done on his behalf using his ID by the scammers from *Bikipro*.

The Complainant further noted that he is now aware that scam trading companies are using crypto exchanges on a regular basis to siphon the savings of innocent

people. He submitted that this gives them the opportunity to launder money, cover their traces and go scot-free.

The Complainant submitted that his issue with *Crypto.com* is based on the fact that Foris DAX has not carried out enough due diligence whilst indirectly accepting him as a client. He noted that even though he never willingly signed up, he was considered their client as his funds were transferred through their platform.

The Complainant further noted that he had no idea back then that the money that was being transferred utilizing the services of *Crypto.com* will never reach his so-called trading account, but instead went directly to the scammers' wallets.

The Complainant claimed that *Crypto.com* did not carry enough due diligence in his case and never warned him that his funds were being transferred to an anonymous wallet.

He submitted that *Crypto.com* neglected the implementation of AML, KYC, and CFT policies while sending his money to scammers. He questioned what if his funds were sent to a terrorist organization or drug sellers.

The Complainant noted that he tried to resolve the issue directly with *Crypto.com* and asked them to reverse his transactions, but he was brushed off and they shifted liability.

A copy of the comprehensive and detailed formal complaint dated 7 September 2021 made by the Complainant with the Service Provider was also attached to the Complaint Form.¹

The Complainant also attached to his Complaint extensive documentation, including, *inter alia*, copies of his bank statement,² evidence of the transactions made with the platforms,³ and extracts of the communications he exchanged with the alleged scammers.⁴

In his formal complaint with the Service Provider, the Complainant explained *inter alia* the following:

¹ P. 7-13

² P. 14 - 25

³ P. 26 - 83

⁴ P. 84 - 249

- That he was a victim of fraudulent activity committed by a scam company, *Bikipro88*, using the *Crypto.com* exchange platform;
- That he was lured and manipulated into investing a total amount of EUR13,957.04 with the account managers of the scam company convincing him to invest more, blackmailing and abusing him, and still trying to extort more money from him;
- That all began when he was contacted via Facebook by a person who convinced him to invest in the *Bikipro88* platform and who kept pushing him to invest more and more until he suspected that the transactions might be fraudulent. He realized this when he attempted several times to withdraw his so-called profits but never succeeded.
- That he searched for information about *Bikipro88* and discovered that many people were scammed by these fraudsters. He noted that *Bikipro88* was an unlicensed and unregulated forex broker which was trying to mislead the customers by presenting itself as a licensed forex broker;
- That regulatory bodies are requiring staunch anti-money laundering ('AML') legislation to prevent money laundering through cryptocurrency exchanges and custodian services. He claimed that when funds were transferred to *Crypto.com* he received no bank alerts as this transaction looked safe to the bank. However, when his funds were sent to the fraudulent company, which steals money from every possible person, he got no warnings whatsoever from *Crypto.com*;
- That due to money laundering policy, *Crypto.com* was obliged to check transactions and block them not to reach the fraudster's wallet;
- That clients like the Complainant cannot understand if a party is manipulating them and stealing their money unless someone from the Service Provider's support team explains why he should not transfer his funds;
- That he contacted the fraud company to try to get his money back but there was no proper response, and they were insisting that he makes further transactions to try to extort more money from him;
- That the Service Provider did not recognize the suspicious activity and did not contact him, warn him, or stop any of the transactions;

- That he felt that his trading account with *Crypto.com* was seriously mishandled and that the Service Provider breached regulations. He was accordingly holding the Service Provider responsible for his lost funds;
- That he was aware that the cryptocurrency field, in general, lacks proper regulation and was still in its first steps, and for this reason, he believed that both the crypto companies and the banking system shared the common problem of lack of preventive methods mostly based on fraud protection and AML policies on the existing and outdated regulatory codes;
- That he was aware that by utilizing blockchain, crypto companies can track bitcoin transactions and investigate and apply all necessary technical processes needed to recover/freeze funds lost to scams and mark the wallet as fraudulent, sometimes freezing the whole Merkle tree. He further noted that the KYC process as well as the blockchain system, using proof of work, verifies all the clients and their transactions to make this possible;
- That *Bikipro88* committed criminal felonies, involving blackmail, misappropriation, and money laundering;
- That fraudsters keep their funds on *Crypto.com* and defraud people utilizing the services of *Crypto.com* with impunity. He alleged that *Crypto.com* closes an eye on enormous amounts of money going through their platform every day despite their KYC and AML policies;
- That a new industry voluntary code was developed for authorized push-payment (APP) scam victims by the *APP Scams Steering Group* which code aimed to protect customers by reimbursing them if they fall victim to an APP scam. Bank customers who were conned into sending money to fraudsters' accounts should find it easier to get compensation after various banks signed up to this code;
- That as a regulated crypto exchanger, the Service Provider should control and block transactions for breaches by the supplier. Reference was made to the Consumer Credit Act, 1974, sections 12(b)/(c) regarding claims against the supplier in respect of a misrepresentation or breach of contract;

- That international and local regulations required *Crypto.com* to implement effective internal procedures/mechanisms to prevent money laundering and other criminal activities taking actions in case of suspicious activity;
- That *Crypto.com* breached the duty of care owed by a financial institution to its clients where there are reasonable grounds to suspect that the sole purpose of a payment instruction is to defraud the client;
- That *Crypto.com* was obliged to refrain from executing the payment instruction until it was able to clarify the legitimacy of the transaction through investigation or further clarification with the client;
- That *Crypto.com* sought no adequate information and documentation at best and at worst implemented no appropriate safeguards;
- That by not utilizing, in a systematic and effective manner, the tremendous amount of data it possessed in order to pinpoint irregular and suspicious activities, the Service Provider was misleading its customers who had taken the leap of faith and placed trust and confidence in its honesty, authority, and competence;
- That the pattern of the disputed transactions was sufficiently suspicious and should have been flagged and blocked by the Service Provider's staff. The Complainant further claimed that no preventive or proactive measures were taken by the Service Provider to protect his financial interests;
- That the Complainant was aware that crypto exchangers have access to a list of suspicious wallets that were being used by scammers all over the world. Therefore, he had reason to believe that the Service Provider deliberately allowed his transactions with the scammers to proceed.

Remedy requested

The Complainant noted that due to *Crypto.com*'s utter negligence and incompetence committed in his case, he is requesting the Service Provider to refund him the total amount that was stolen from him in respect of which *Crypto.com* acted as an intermediary. This amounts to EUR13.957,04.⁵

⁵ P. 3

In its reply, Foris DAX MT Limited essentially submitted the following:⁶

That *Foris DAX MT Limited* ('Foris DAX' or 'the Service Provider'), previously known as *MCO Malta DAX Limited*, is licensed as a Class 3 VFA Service Provider by the MFSA.

That Foris DAX offers a crypto custodial wallet ('the Wallet') and the purchase and sale of digital assets on own account, through the *Crypto.com* App. The Wallet is only accessible through the App and the latter is only accessible via a mobile device.

That the Complainant became a customer of Foris DAX through the *Crypto.com* App on 5 June 2021.

The following timeline was provided by the Service Provider:

- a) 11 June 2021 – The Complainant purchased the amount of 0.075 ETH (Ethereum) in exchange for Eur150.51 through the *Crypto.com* App using his personal debit/credit card to complete the transaction.

Later, on the same day, the Complainant transferred the total amount of 0.0664 ETH from his Wallet to an unknown external wallet address. A screenshot was provided of the said purchase and transfer.⁷ The transaction was successfully executed and a withdrawal transaction fee of 0.008 ETH was debited from his Wallet.

- b) 15 June 2021 – The Complainant purchased the amount of 0.47 ETH (Ethereum) for Eur1,006.43 through the *Crypto.com* App using his personal debit/credit card to complete the transaction.

Subsequently, the Complainant transferred the total amount of 0.460406327947747 ETH from his Wallet to an unknown external wallet address.

The transaction was successfully executed and a withdrawal transaction fee of 0.008 ETH was debited from his Wallet, as per the screenshots provided.⁸

⁶ P. 367-373

⁷ P. 368

⁸ *Ibid.*

- c) 26 June 2021 – The Complainant purchased the amount of 0.68 ETH (Ethereum) in exchange for Eur1,001.57 through the *Crypto.com* App using his personal debit/credit card to complete the transaction.

Later on the same day, the Complainant transferred the total amount of 0.662 ETH from his Wallet to an unknown external wallet address. A screenshot was provided of the said purchase and transfer.⁹ The transaction was successfully executed and a withdrawal transaction fee of 0.008 ETH was debited from his Wallet.

- d) 7 July 2021 – The Complainant purchased the amount of 0.51 ETH (Ethereum) in exchange for Eur1,034.86 through the *Crypto.com* App using his personal debit/credit card to complete the transaction.

Later on the same day, the Complainant transferred the total amount of 0.512 ETH from his Wallet to an unknown external wallet address. A screenshot was provided of the said purchase and transfer.¹⁰ The transaction was successfully executed and a withdrawal transaction fee of 0.008 ETH was debited from his Wallet.

- e) 19 July 2021 – The Complainant purchased the amount of 3 ETH (Ethereum) across two separate purchases in exchange for Eur4,849.52 through the *Crypto.com* App using his personal debit/credit card to complete the transaction.

Later, on the same day, the Complainant transferred the total amount of 2.923567 ETH from his Wallet to an unknown external wallet address. A screenshot was provided of the said purchase and transfer.¹¹ The transaction was successfully executed and a withdrawal transaction fee of 0.008 ETH was debited from his Wallet.

- f) 20 July 2021 – The Complainant purchased the amount of 0.5235 ETH (Ethereum) across two separate transactions in exchange for Eur823.63 through the *Crypto.com* App using his personal debit/credit card to complete the transaction.

⁹ P. 369

¹⁰ *Ibid.*

¹¹ P. 370

Later, on the same day, the Complainant transferred the total amount of 0.577858142737128 ETH from his Wallet to an unknown external wallet address. A screenshot was provided of the said purchase and transfer.¹² The transactions were successfully executed and a withdrawal transaction fee of 0.008 ETH was debited from his Wallet.

- g) 26 July 2021 – The Complainant purchased the amount of 0.71 ETH (Ethereum) in exchange for Eur1,489.03 through the *Crypto.com* App using his personal debit/credit card to complete the transaction.

Subsequently, the Complainant transferred the total amount of 0.697352221045357 ETH from his Wallet to an unknown external wallet address. A screenshot was provided of the said purchase and transfer.¹³ The transaction was successfully executed and a withdrawal transaction fee of 0.008 ETH was debited from his Wallet.

- h) 27 July 2021 – The Complainant purchased the amount of 0.4 ETH (Ethereum) in exchange for Eur789.84 through the *Crypto.com* App using his personal debit/credit card to complete the transaction.

Later in the same day, the Complainant transferred the total amount of 0.392 ETH from his Wallet to an unknown external wallet address. A screenshot was provided of the said purchase and transfer.¹⁴ The transaction was successfully executed and a withdrawal transaction fee of 0.008 ETH was debited from his Wallet.

- i) 31 July 2021 – The Complainant purchased the amount of 1.3 ETH (Ethereum) in exchange for Eur2,811.65 through the *Crypto.com* App using his personal debit/credit card to complete the transaction.

Later in the same day, the Complainant transferred the total amount of 1.292 ETH from his Wallet to an unknown external wallet address. A screenshot was provided of the said purchase and transfer.¹⁵ The transaction was successfully executed and a withdrawal transaction fee of 0.008 ETH was debited from his Wallet.

¹² P. 370

¹³ P. 371

¹⁴ *Ibid.*

¹⁵ P. 372

In total, the Complainant purchased the amount of 7.6685 ETH in exchange for Eur13,957.04 across 11 individual transactions taking place between the 11 June 2021 and 31 July 2021.

- j) 8 September 2021 – The Complainant sent the *Crypto.com* Customer Service Team a letter detailing that he has been the victim of a scam and was coerced to send the above-mentioned ETH amounts to a ‘scam company’. The Complainant requested a full refund of the Eur13,957.04 he personally sent to a third-party wallet after purchasing digital assets in exchange for the amount in Euros through the *Crypto.com* app.
- k) 16 September 2021 – The Complainant sent the *Crypto.com* Customer Service Team a follow up letter in which he reiterated his request for a refund of the Eur13,957.04 through the *Crypto.com* app. A copy of the demand letter and communications between the Complainant and the Customer Service Team were attached.
- l) 18 September 2021 – The case was forwarded to the *Crypto.com* Complaints Team who provided the Complainant with a final reply.

After carefully reviewing and reassessing the Complainant’s case, the team issued an official response that it cannot offer a reimbursement of the transfers the Complainant executed himself from his Wallet to an external wallet address. *Crypto.com* cannot revoke any virtual asset withdrawals as transactions done on the blockchain are immediate and immutable. The Complainant was also advised that Foris DAX cannot be held responsible for the Complainant’s personal decisions and actions, which led to the unfortunate event of him transferring his virtual asset holdings to an ill-intended third party.

The Service Provider submitted that the Complainant is solely responsible for the security and authenticity of all instructions submitted through his Wallet and the *Crypto.com* App as outlined in its Terms of Use, an extract of which was provided as follows:

‘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, the Service Provider submitted that it seems possible that the Complainant has been the victim of an alleged scam and has voluntarily, according to his own statements, transferred his ETH virtual asset holdings from his *Crypto.com* Wallet to external wallet addresses he has no access to.

The alleged owner of the said external wallet addresses has allegedly refused to cooperate with the Complainant and return his crypto assets. As outlined in Foris DAX Terms of Use, the Complainant is solely responsible for the security and authenticity of all instructions submitted through the *Crypto.com* app.

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 555¹⁶ which stipulates that he should deal with complaints in ‘*an economical and expeditious manner’*.

The Complainant and his crypto account

The Complainant, who is resident in the Netherlands, became a customer of Foris DAX on 5 June 2021 through the *Crypto.com App*, as confirmed by the Service Provider.¹⁷

¹⁶ Art. 19(3)(d)

¹⁷ P. 367, 694 & 700

The disputed transactions undertaken from the account held with Foris DAX, according to the transaction history provided by the Complainant, are as follows:

- a) 11 June 2021 - Bought 0.075 ETH @ €150.51. Withdrew 0.0744 ETH;¹⁸
- b) 15 June 2021 - Bought 0.47 ETH @ €1,006.43. Withdrew 0.468406327947747 ETH;¹⁹
- c) 26 June 2021 - Bought 0.68 ETH @ €1,001.57. Withdrew 0.67 ETH;²⁰
- d) 7 July 2021 - Bought 0.51 ETH @ €1,034.86. Withdrew 0.52 ETH;²¹
- e) 19 July 2021 - Bought 1.5 ETH @ €2,354.18 and another purchase of 1.5 ETH @ €2,354.55. Withdrew 2.931567 ETH;²²
- f) 20 July 2021 - Bought 0.41 ETH @ €625.27. Withdrew 0.467398570935943 ETH. Bought 0.1135 ETH @ €174.44. Withdrew 0.126459571801185 ETH;²³
- g) 26 July 2021 - Bought 0.71 ETH @ €1,445.80. Withdrew 0.705352221045357 ETH;²⁴
- h) 27 July 2021 - Bought 0.4 ETH @ €766.91. Withdrew 0.4 ETH;²⁵
- i) 31 July 2021 - Bought 1.3 ETH @ €2,730.02. Withdrew 1.3 ETH.²⁶

During the indicated one-and-a-half-month period from 11 June till 31 July 2021, the Complainant bought and transferred ETH over several transactions.²⁷

The withdrawals were done to external wallet addresses provided by the alleged scammer as testified by the Complainant during the hearing of 29 March 2022 where he stated

*‘that there were a number of trades during this period that I had the relationship with Bkipro. They sent me three Wallets. I sent them to three external Wallets from Crypto’.*²⁸

¹⁸ P. 26

¹⁹ *Ibid.*

²⁰ *Ibid.*

²¹ *Ibid.*

²² *Ibid.*

²³ P. 27

²⁴ *Ibid.*

²⁵ *Ibid.*

²⁶ *Ibid.*

²⁷ In exchange, in total, for over EUR13,600. According to the said extracts a slight discrepancy of €312.50 results from the figure of €13,957.04 indicated in the Complaint Form (P.3) and in the Service Provider’s reply (P. 372). The said discrepancy however does not affect in any way the decision outlined in this case.

²⁸ P. 363

The disputed transactions were done by the Complainant himself. During the hearing of 29 March 2022, the Complainant confirmed *inter alia* that

'I started buying Ethereum because I wanted to invest in that platform' [of Bkipro].²⁹

He further testified, during the same hearing, that *'I confirm that I purchased Ethereum via my credit card on the crypto exchange, and transferred to a third party Wallet'.³⁰*

The Service Provider

Foris DAX MT Limited ('Foris DAX' or 'the Service Provider') is a company registered in Malta on 19 September 2018 with Company Registration Number C 88392 as per the records held with the Malta Business Registry.³¹

Foris DAX MT is licensed by the Malta Financial Services Authority ('MFSA') as a VFA Service Provider as per the MFSA's Financial Services Register.³² 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.³³

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'.³⁴*

²⁹ P. 362

³⁰ *Ibid.*

³¹ <https://registry.mbr.mt/ROC/index.jsp#/ROC/companiesReport.do?action=companyDetails&fKey=ab2b4261-837f-4d91-8547-e97ed3935ef2>

³² <https://www.mfsa.mt/financial-services-register/>

³³ <https://www.mfsa.mt/financial-services-register/>

³⁴ <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 ...’.³⁵

It offers the account holder ‘a crypto custodial wallet’ and ‘the purchase and sale of digital assets on own account’.³⁶

Observations & Conclusion

Summary of main aspects

The Complainant made various transfers of his digital asset (ETH) using the *Crypto.com* app. The said transfers were made to external wallet addresses allegedly used by a fraudster. The transfers were in respect of a fraudulent trading platform as explained by the Complainant in his Complaint³⁷ and testified during the hearing of 29 March 2022.³⁸ The Complainant realised that the third-party trading platform was a scam when he tried to withdraw money ‘but never succeeded’.³⁹

In essence, the Complainant is seeking reimbursement 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 Foris DAX failed to carry out enough due diligence, failed to adhere to anti-money laundering (AML), know your client (KYC), and countering the financing of terrorism (CFT) requirements and never warned him about transfers to anonymous wallets.⁴⁰ The Complainant also stated that he asked the Service Provider to reverse his transactions, but the Service Provider brushed him off and shifted liability.

On its part, Foris DAX is, in essence, claiming that it has no responsibility for the payments 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

³⁵ P. 623

³⁶ P. 367

³⁷ P. 2 & 7

³⁸ P. 363

³⁹ P. 7

⁴⁰ P. 2 & 3

it was not possible for Foris DAX to revoke or reverse the crypto withdrawal once the transactions were done on the blockchain.

As also testified by an official of the Service Provider during the hearing of 23 May 2022,

*'It is also important to note that cryptocurrency transactions and the technology in which it works in, are very different from the traditional form of banking. Cryptocurrency transactions are designed to be irreversible; and the service provider does not have any control over them after they have been properly authorised.'*⁴¹

The Service Provider further stated during the same hearing that:

*'We would also highlight that although the complainant alleges that he had no access to the so-called "third-party wallets", there is no way for us to provide this. The ability to anonymously operate is an important element to cryptocurrency transactions. What we can do is to track which account these monies were sent to but we are unable to verify the ownership of each and every one of these accounts if they are not a Crypto.com account itself. One person can hold multiple addresses without any apparent link between the addresses and the indication of who holds it'.*⁴²

Applicable Regulatory Framework

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

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

⁴¹ p. 695

⁴² *Ibid.*

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'* ⁴³ 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').

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.

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 relates to payments made by the Complainant, from his account held with Foris DAX, to an allegedly fraudulent external trading platform.

The Complainant expected the Service Provider to prevent, stop or reverse his transactions. He claimed that the Service Provider had *'never warned [him] that [his] funds are being transferred to an anonymous wallet'*, had *'neglected the implementation of AML, KYC and CTF policies'* and *'not carried enough due diligence'*.⁴⁴

He further claimed that when he asked Foris DAX to reverse his transactions, the Service Provider brushed him off and shifted liability.⁴⁵

⁴³ Guidance 1.1.2, Title 1, *'Scope and Application'* of the *'Guidance on Technology Arrangements, ICT and Security Risk Management, and Outsourcing Arrangements'*.

⁴⁴ P. 2 & 3

⁴⁵ P. 3

The Arbiter however considers that no adequate and sufficient evidence has emerged to substantiate the claims made against the Service Provider. This is also given the nature of the transactions which involved crypto assets, the type of service provided, and other reasons as outlined below.

- The Complainant opened his account on 5 June 2011. The disputed transactions commenced a few days later on 11 June 2021, and continued over a one-and-a-half-month period till the end of July 2021, as further outlined above in the section titled *'The Complainant and his crypto account'*.

Given the limited transaction and operating history of the account held with *Crypto.com* and the nature of the transactions in question involving purchases and transfers of crypto, the Arbiter does not accordingly consider there is sufficient basis to suggest that the transactions were out of character and necessitated the immediate intervention of the Service Provider.

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.

- It has, furthermore, not been demonstrated nor emerged that the alleged fraudster to whom the various payments were 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 *'external wallets'* and, hence, the Service Provider had no information about the third party to whom the Complainant was transferring his crypto.⁴⁶
- The Arbiter is not satisfactorily convinced either that a warning by the Service Provider in relation to the dangers associated with transfers to an anonymous wallet, as suggested by the Complainant, would have stopped the Complainant from proceeding with the disputed transactions.

⁴⁶ P. 105

Whilst such a warning could have been helpful and is indeed recommendable, however, the Arbiter does not have sufficient comfort that this would have stopped the Complainant from proceeding with the transfers.

This is when taking into consideration the sophisticated nature of the scam perpetrated by the scammer where the Complainant was craftily groomed over a period of time by the fraudulent party to invest in a fake platform.

The Arbiter also notes that the scam was so elaborate and deceiving that, unfortunately, the Complainant had not stopped with the transfers despite the reservations raised by his family and friends, as emerging from the extracts of the chats the Complainant had on 23 June 2021 with the scammer.⁴⁷

- The Complainant contacted the Service Provider on 8 September 2021,⁴⁸ by which time the transactions had long been completed and finalized.⁴⁹

Once a transaction is complete, and accordingly is not in a pending state, the crypto transaction cannot be cancelled or reversed as provided for and warned in the Terms and Conditions of Foris DAX⁵⁰ (and as typically also indicated on various other internet sites).⁵¹

As also indicated by the Service Provider, Clause 7.2(b) of its Terms and Conditions regarding the use of the Crypto.com App Services specifically states 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...'*⁵²

⁴⁷ P. 190

⁴⁸ P. 375

⁴⁹ Crypto transactions may be processed and completed within a few minutes or hours (as indicated on various websites following a general search on the internet).

⁵⁰ Clause 3.1 and Clause 7.2(b) of the Terms and Conditions on the use of the Crypto.com App Services (P. 651-659).

⁵¹ E.G. <https://www.chargebackgurus.com/blog/chargebacks-more-volatile-complex-than-cryptocurrency>

⁵² P. 659 – Emphasis added by the Arbiter

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:⁵³

‘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.’

- **The Arbiter also notes that in his Complaint filed with the Office of the Arbiter for Financial Services, the Complainant referred to the AML, CFT, and KYC policies that the Service Provider was subject to.**

The Arbiter considers that the AML provisions referred to by the Complainant do not support or justify in any way his claims for compensation under Chapter 555 of the Laws of Malta. As outlined above, it has not been demonstrated nor emerged that the transfer was made to another *Crypto.com App* user in the first place and hence the context of the quoted AML requirements is inapplicable.

The industry code for APP victims (which is voluntary for financial institutions in the UK), and the quoted Consumer Credit Act applicable in the UK are similarly not applicable to the Service Provider as an entity based in Malta.

It is also to be noted that Foris DAX is regulated and licensed as a VFA Service Provider as outlined above. Foris DAX is itself not a financial institution, and the regulatory regime applicable to a VFA Service Provider is a different one from that applicable to a financial institution falling under EU regulatory regimes.⁵⁴

⁵³ P. 660

⁵⁴ 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).

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, either contractually and/or arising from the VFA regulatory regime applicable in respect of its business.

- The Complainant produced over 100 pages of chats he had with the scammer.⁵⁵ These show how he was groomed by the scammer over a period of time, where the scammer slowly earned his trust despite the Complainant being initially skeptical.

The Complainant was eventually persuaded to transfer a low amount of digital assets for the purported trading, with the scammer guiding the Complainant on how to make trades on a spoof trading platform that indicated fictitious profits. The fake trades, which the Complainant thought were real ones, were executed multiple times during June and July 2021. During such time, the Complainant kept being pushed by the scammer to deposit more and higher amounts to trade.

Along the process, the Complainant was not just persistently pushed by the scammer to put his own cash for the purported investment but also persistently encouraged to get loans by any means possible - against his personal assets and also from his family, friends, and colleagues.

The scammer eventually kept trying to extract money from the Complainant by continuously asking for new payments (such as in tax and withdrawal fees) to be settled prior to the supposed release of his capital together with his fictitious profit, only for withdrawals never to be realized despite the settlement of requested payments.

It is clear that the Complainant has unfortunately fallen victim to a cruel and sophisticated scam, which type of scams are alarmingly estimated to have caused billions in losses to victims worldwide in 2021 alone.⁵⁶

⁵⁵ P. 136-249

⁵⁶ <https://www.forbes.com/sites/cyrusfarivar/2022/09/09/pig-butcherer-crypto-super-scam/?sh=5c1dafafec8e>

Decision

The Arbiter sympathizes with the Complainant for the ordeal he suffered as a victim of a cruel scam. Given the particular circumstances of this case, the Arbiter cannot however accept his request for compensation for the reasons amply mentioned in this decision. The Complaint cannot accordingly be upheld.

Since cryptocurrency is a relatively new area, the Arbiter would like to make a few observations.

The increasing and alarming volume of scams and fraud existing in the crypto field, as emerging from recent statistics, is of great concern.⁵⁷ Such scams and fraud are leaving devastating effects on many retail customers and their families.

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

Consumers need to, more than ever, be extra vigilant and take appropriate and increased measures to safeguard themselves to avoid and minimise the risk of falling victims.

Genuine service providers can also actively contribute to improving the consumers' awareness of the particular risks, including, fraud and scam education, relevant to this sector.

Given the extent of scams and fraud which is disturbingly emerging, and the devastating implications left by such, service providers are also strongly encouraged to voluntarily devise enhanced mechanisms to mitigate the occurrence of customers falling victims and how victims of scams and fraud can be better helped and supported in the crypto field. Through their status and

<https://www.ft.com/content/5987649e-9345-4eae-a4b8-9bfb0142a2ab>

⁵⁷ <https://blog.chainalysis.com/reports/2022-crypto-crime-report-introduction/>

<https://www.ftc.gov/news-events/data-visualizations/data-spotlight/2022/06/reports-show-scammers-cashing-crypto-craze>

moral obligations, main providers in the crypto field can initiate and bring an improved standard of consumer protection in this industry.

Given the particular circumstances and novel nature of this case, each party is to bear its own legal costs of these proceedings.

**Dr Reno Borg
Arbiter for Financial Services**