Before the Arbiter for Financial Services

Case ASF 084/2026

UT

('the Complainant')

vs

Foris DAX MT Limited

(Reg. No. C 88392)

('Foris' or 'Service Provider')

Sitting of 23 September 2026

The Arbiter,

Having seen the Complaint dated 06 March 2026 made against Foris DAX MT Limited relating to its alleged failure to refund €25,400 being two payments made from his account with Foris without being authorised by him.

The Complaint[1]

In his complaint form to the Office of the Arbiter for Financial Services ('OAFS'), the Complainant submitted that at the time of the incident, his device was compromised via remote access (device takeover) so that although from the point of view of Foris these payments appeared properly authorised by him, in actual fact these payments were made by fraudsters to whom he had unknowingly granted access through the *AnyDesk* application.

He stated:

[1] P. 1 - 6 with supporting documentation on P. 7 - 58

I suffered financial losses of EUR 12,500 and EUR 12,900 due to unauthorized transactions on my Crypto.com account. These transactions were not authorized by me

No police report is available. The fraud was reported to the financial service providers involved.

At the time of the incident, my device was compromised via remote access (device takeover). In such fraud scenarios, the attacker uses the already authenticated session without changing credentials, which makes the activity appear as if performed by the legitimate user.

Crypto.com rejected my complaint based solely on the absence of credential changes and the use of the same session, and, later issued a final position. I believe Crypto.com failed to properly investigate the correct fraud scenario (device takeover) and misclassified the case as user fault.

…..

I seek reimbursement of the financial loss resulting from the unauthorised transactions, or any other remedy the Arbiter deems appropriate"[2].

The payments in question were effected as follows:

Date	**Amount in EURO**	**Ref.**	**Exchanged into ETH and transferred out**	**Ref.**
11.08.2025	12,500	p. 34	3.22328	p. 64
20.08.2025	12,900	p. 32	3.438232	p. 64
Total	**25,400**		**6.661512**	

[2] P. 3

The transfers out were effected on 13 and 21 August 2025[3] to a linked account referred to as a Crypto Exchange with a related company Foris DAX Limited registered in the Cayman Islands.

By way of resolution, he seeks refund of the payments effected without his authority '*which disappeared from my Crypto.com* (brand name of Foris) *account, or any other remedy the Arbiter deems appropriate.*[4]'

Service Provider's reply

Having considered in its entirety, the Service Provider's reply[5] where the Service Provider provided a summary of the events which preceded the Complainant's formal complaint and explained and submitted the following:

1. *Background*

- ***"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 "Cash Wallet") (formerly referred to as the Crypto.com Fiat (EUR) Wallet), which allows customers to top up and withdraw fiat currencies from and to their personal bank account(s). This service is offered by the legal entity Foris MT Limited.***

- ***Foris DAX Limited, a company registered in the Cayman Islands, offers the services of the Crypto.com Exchange (the "Exchange"). The Crypto.com Exchange is a separate centralized, high-performance cryptocurrency trading platform designed for advanced users.*** [6]***"***

The Service Provider then provided a timeline for the transactions of the Complainant's account with them. These included above listed inward transfers

[3] P. 85
[4] P. 3
[5] P. 62 - 70 with attachments from p. 71 - 75
[6] P. 62

of Euro fiat currency. These funds were then converted to crypto assets (ETH)[7] and transferred out to Complainant's Exchange wallet with a related company trading under same brand, Crypto.com.

They maintain that Complainant first informed Foris of his case on 03 October 2025, and his wallet was temporarily disabled and his complaint considered by their risk team as a potential account takeover. Following analysis of information given by Complainant through an Account Takeover questionnaire, the claim for refund was declined.

> ***"Our internal investigation provided a clear and unequivocal indication that the Complainant had wilfully; or by way of negligence in regard to the privacy and security of his mobile device and personal credentials, involuntarily facilitated the alleged unauthorised access to his Wallet.***
>
> ***Please find additional context in support of said decision below:***
>
> ***• Our audit trail shows that no change of passcode or login credentials, or any failed login attempts have been registered for the Wallet of the Complainant, 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.***
>
> ***Kindly note that as outlined in the Foris DAX MT Limited Terms of Use, the Complainant is solely responsible for maintaining adequate security and control of his mobile device as well as login and authentication details. I have further shared the relevant part of the Terms of Use accepted by the Complainant for your reference:***
>
> ***QUOTE***
>
> ***6. YOUR DEVICE***
>
> ***…***
>
> ***6.2 Without prejudice to the foregoing and any other terms in these Terms, we assume that any and all Instructions received from your Enabled Device have been made by the rightful owner. You are solely***

[7] ETH is abbreviation for Ethereum, a popular digital asset

responsible and liable for keeping your Enabled Device safe and maintaining adequate security and control of your login and authentication details (including, but not limited to, your username, and password), and shall likewise be solely responsible for any access to and use of the Crypto.com App Services or Crypto.com Web Services through your Enabled Device, notwithstanding that such access and/or use may have been effected without your knowledge, authority or consent. We will not be liable to you for any loss or damage resulting from such access and/or use.

UNQUOTE

The assessment of the "Account Takeover" case was completed by the Risk team and their decision provided to the Complainant via email on January 16, 2026."[8]

Foris then quoted exchanges with Complainant informing of their decision and subsequent exchanges following protests and appeals by Complainant to have their decision reviewed[9].

They noted that Complainant had admitted that his personal device was controlled by fraudsters via AnyDesk, a remote access software. They emphasised that such software requires two-factor verification, requiring the user to provide their PIN and password for another individual to gain access to their device. They concluded:

> ***"In summary, while we fully empathize with (Complainant), Foris DAX MT Limited respectfully submits that it bears no responsibility for any loss suffered. As stated previously, our audit trail shows no change of passcode or login credentials and no failed login attempts registered with regards to the Complainant's Crypto.com account at the material time. Moreover, the Complainant verified that his device had been remotely controlled via AnyDesk, an action which necessitates explicit user authorization to grant access.***

[8] P. 67
[9] P. 68 - 70

> ***Kindly note that the Company is unable to reverse any of the transactions performed through the Complainant's Wallet since transactions done on the blockchain are immediate and immutable.***
>
> ***We remain at your disposal for any further information you may require pertaining to the above case."***[10]

Hearings

At the first hearing on 02 June 2026, the Complainant reiterated he did not authorise the two payments in question and denied knowingly giving remote access to the fraudster by AnyDesk software.

Under cross-examination he said:

> ***"I am referred to my complaint where I say that the incident is referred to as an account takeover, I say, yes.***
>
> ***Asked whether it is correct to say that at the time of the incident, my account was initially accessed by me, and that I inserted my credentials and my passcodes and, therefore, during that time where I had accessed my own account, that is when the transactions took place, I say, yes.***
>
> ***Asked whether I had an app called AnyDesk installed on my laptop, I say, yes, but that access was obtained through deception and social engineering. I did not knowingly authorise cryptocurrency transfers or withdrawals.***
>
> ***Asked whether I had installed the app, AnyDesk, I say, yes.***
>
> ***I did not know what AnyDesk was. So, the problem is that, I did not click on AnyDesk because I did not know about AnyDesk. The hacker used my computer and used the AnyDesk app, but it was not on my computer. I didn't know anything about AnyDesk.***
>
> ***So, I think he made an installation of that or something. And the provider could see things I could not, and choose total denial over any shared responsibility. A regulated platform has a transaction visibility.***

---

[10] P. 70

It is said that the question is whether I had the app, AnyDesk, and I confirmed that I did have that app, AnyDesk, on my laptop.

Asked whether I had an application called AnyDesk installed on my device as on page 10 of my complaint, I say, at the time of the incident, my computer was compromised via remote access software AnyDesk, I say that my son said that AnyDesk was installed by the hacker.

So, it is said that I did have the app, AnyDesk, installed on my device.

I say, I think so.

It is said that according to the reply of the Service Provider, these transactions were made on the 15th of August and the 28th of August.

Asked whether it is correct to say that I first contacted the Service Provider on the 3rd of October, I say that I had daily contact with Crypto.com with the Customer Department where I reported that my money was conned on the account. So I can prove that also because there are a lot of e-mails I had sent to the Service Provider. And I have waited for three and a half months with Crypto.com saying that it is under investigation.

Probably, I sent more than one hundred messages asking what was happening and asking where my money was. And it took three and a half months before I had a decent reaction from Crypto.com.

So I can prove that because I can send the emails from the end of August to the beginning of September.

It is said that, according to the reply of the Service Provider, I contacted the Crypto.com customer support on the 3rd of October 2025.

I say, no, no, no, no, the end of August, madam. Not in October. I already reported the end of August to Crypto.com customer service. First, you get a robot, and then you can speak to the specialist.

And I did that already in the last days of August. I don't know what you mean, because you're not well informed. There are files at Crypto.com, I suppose.

It is said that, according to the information, which is just a track, where there is a whole trail of my correspondence; the first time that I actually reached customer support was on the 3rd of October 2025 as indicated in the reply of the Service Provider.

I say that it was the end of August.

It is said that I did not submit any evidence to show otherwise.

I say that I can prove it to you.

It is said that all withdrawals were made from my exchange account.

Asked whether this is correct, I say, I don't know what an exchange account is.

It is said that these withdrawals I am talking about were made to my exchange account with Foris DAX.

Asked whether this is correct, I say, I am sorry, but I don't know what this is all about. I did not do anything, booked or did something on my account. The money just disappeared, nothing more than that.

I am referred to what I said that two withdrawals that I could not see, were made on the 15th and 28th August.

Asked whether this is correct, I say, yes.

It is said that these withdrawals were made to my Exchange account.

I say, yes.

It is said that the Exchange account is not serviced by Foris, by the company that we have today, but is serviced by Foris DAX Limited.

I say, yes.

It is said that the money allegedly left Open Bank, that there was a transfer from Open Bank.

I say, yes, that's right.

Asked when I realised, or I am saying, that the transactions which were unauthorised were made from Open Bank, whether I contacted Open Bank to tell them that, I say, yes, of course.

They told me that they had received the details that they told me that they made the booking to my Crypto.com account, and that they could not do anything about it.

I did not make the booking online, but directly, speaking on the telephone to, Open Bank. So, they confirmed and made the booking in two parts: €12,500 and €12,900. And I could see on the dashboard that the amounts of €12,500 and €12,900 had arrived at Crypto.com.

The Arbiter asks me whether I authorised the transfer from my bank, Open Bank, to Crypto.com, I say, yes, I did.

Asked what was the purpose of opening a Crypto.com account and making the deposits, I say that I thought that there is a very low rate in Avante. When you have a savings account, you get 1% or something. So, I thought, when I booked it to the Crypto.com, I can earn a better rate because you can change it to another crypto, Ethereum or something like that. And, then, you can make more money because when you change it at the moment when the Ethereum or Bitcoin is high, you can earn more than 1%. So that was the reason for me to book to Crypto.com.

Asked whether my son was helping me operate this account, I say, no, no. The problem is that they didn't know anything about it, so they were very angry that I lost the €26,000, and asked how that was possible and how did I do that.

After investigating, my son found out that my computer was four months under the control of the hacker.

So later, in the end of October, €4,000 disappeared from my Dutch bank account. I think that's the same hacker, of course.

Asked how I came to learn about trading in cryptocurrencies, I say that I didn't know anything about it. I had the intention, when I booked the amounts on Crypto.com, of asking a specialist.

For instance, I should have asked my son what is the best way to invest there, but I didn't ask him in the first place, and later it was too late. I saw a few days later that the bank account balance was zero. The money has disappeared.

I am asked what I meant when I told the Customer Service on the 3rd of October, 'I have a financial advisor who helps me but now I do not see the amount on my account anymore.'

Asked who my financial advisor is, I say that now, I have no financial advisor. I asked my son, when you have a dashboard, you see the money is coming in. You also have to see when the money is going out. And on the dashboard, there was nothing to see. You are making a big mistake. You already said already that I made contact in October, but I made contact at the end of August. I had very much contact with Crypto.com's customer service about this. So, please, stop saying this.

The Arbiter states that the question was whether I had or I had not a financial advisor.

I say, no, my son was the financial advisor. I never had a financial advisor to do anything with Crypto.com.

Asked why I said that I had a financial advisor, I say, that was my son.

Asked whether the financial advisor was my son who advised me to invest in crypto, I say, no. It was someone else, a friend of mine who was doing well in crypto, said to me, 'You have to do that because you can earn money that way.' So that was the reason I invested the money with Crypto.com.

It is said that then my friend was the financial advisor.

I say, yes, yes, if you would call him a financial advisor."[11]

Following the hearing, Complainant sent a copy of a notice dated 29 August 2025, apparently from Foris, informing that following a routine review, they were restricting his account by blocking any outward transfers of digital assets. He

[11] P. 77 - 81

affirmed that he had already been in contact with Foris about the matter much earlier than 03 October 2025 as they claim.

A second hearing was held on 13 July 2026 for the proofs of the Service Provider who presented Pema Fung to state:

> ***"The Complainant became a client and user of the Service Provider on the 1st of August 2025. The disputed transactions in question relate to two transfers of cryptocurrency, which was purchased using the Complainant's Crypto.com app account and sent to the Complainant's linked Crypto.com exchange account on the 13th of August and the 21st of August, 2025.***
>
> ***We apologise for the error in the Service Provider's reply, which I believe stated an incorrect date of the 6th of April 2025.***
>
> ***As explained in the Service Provider's reply, the Crypto.com exchange is a completely separate cryptocurrency trading platform, which is serviced by Foris DAX Limited, a company registered in the Cayman Islands.***
>
> ***When an exchange account is created and registered with the same e-mail address and telephone number as a Crypto.com app account, the Crypto.com app account or the app, will automatically detect this and enable the exchange account to be linked to the Crypto.com app account. A Crypto.com app account recognizes a user's exchange account because both platforms are linked under the same core ecosystem ID. When an account is registered for the exchange using the identical e-mail and phone number as the app account, the system matches the user's credentials and verifies the shared KYC identity data.***
>
> ***This back-end integration allows a user to instantly link the two services and make free transfers without any fees between their app wallet and the exchange account. From the evidence at hand, the two transfers were fully authorised using the Complainant's login credentials for his Crypto.com app account which remained unchanged throughout the material time. This was either made by the Complainant himself or through his authorised device, which he has admitted to having granted***

access to the Complainant's so-called financial advisor through the installation of AnyDesk software.

There was nothing to show in our own controls, as well as the controls of our third-party monitoring tools to indicate that there was any malicious or scam activity involved in the transactions at the material time.

The Complainant's concerns regarding these transactions were not communicated or brought to the attention of the Service Provider until these transactions had already been completed. And they were simply transfers made to the Complainant's own linked Crypto.com exchange account.

To this the Service Provider submits that we are not responsible for any of the losses suffered by the Complainant in this complaint. [12]***"***

Under cross-examination, Complainant asked why on 29 August 2025, merely 8 days after his last transfer, Crypto.com sent him a warning and restricted his account from further transfers[13]. He asked whether at that point in time Foris was already aware of the fraud. Ms Fung chose to reply in writing after the hearing as she needed time to investigate internally what had led to the warning of 29 August 2025.

On 31 July 2026, Foris informed that:

"It has been verified that the Complainant's account routine review email and the subsequent restrictions (which were applied to both the Complainant's Crypto.com App and Crypto.com Exchange accounts for his account safety) appear to have been triggered by a withdrawal attempt made on 29 August 2025. This withdrawal attempt was made through the Complainant's Exchange account and not through his Crypto.com App account. Consequently, the information relating to the blocked withdrawal is held exclusively by the Exchange service provider and not Foris Dax MT Ltd (the Crypto.com App service provider)."[14]

[12] P. 85 - 86
[13] P. 87
[14] P. 98

Foris also sent evidence that on 13 August 2025, before the two transfers subject of this complaint had been made, they had already stopped two transfers to external wallets and issued a warning about the risks of making transfers to external wallets[15].

Final Submissions

In their final submissions, the parties basically repeated what had already emerged in the complaint, the reply and the hearing proceedings.

Having heard the parties

Having seen all the documents

Considers

This case revolves around whether the Service Provider can be held responsible for the two payments which Complainant considers unauthorised, whilst Foris maintain that these payments were, from their point of view, properly authorised by Complainant. Foris maintain that the Complainant is fully responsible for the loss as he gave access to fraudsters to his account by installing the AnyDesk application, through which fraudsters could operate through a complete takeover of his account.

Complainant's evidence, as quoted above, shows he was in a state of confusion which was exploited by the fraudsters. He admits opening an account with Crypto.com to hold digital assets on the advice of an unidentified friend who made him believe that he could earn higher interest rates, as if a crypto account was like a bank deposit account.

He did not reveal how he was contacted by scammers and why he agreed to install, or let scammers install, the AnyDesk application without having the slightest idea of what was the purpose of such application. He merely refers to access to his account having been obtained by deception and (months of) social engineering[16].

[15] P. 99
[16] P. 76

He states he never involved his son for any technical advice before it was too late and then his son discovered that his computer had been *'four months under the control of the hacker'*[17].

He says he did not know he had an Exchange account where the ETH was transferred but admitted that he knew that withdrawals were made to his Exchange account and that he knew that the Exchange account was not with the Service Provider but with an associated company Foris DAX Ltd[18].

It appears that, apart from the losses claimed under this complaint, he also lost €4,000 which '*disappeared from my Dutch bank account*'[19] indicating that scammers took over also his normal bank account.

He failed to make a report of the fraud to the police in his home country, the Netherlands. He was hiding his 'investments' from his family '*so they were very angry that I lost the €26,000, and asked how that was possible and how did I do that*'[20].

Complainant laid great emphasis during his evidence and in his final submissions that he had been in contact with Foris about this case since the end of August rather than the beginning of October as Foris declared in their reply.

There is no doubt that Foris had informed him that they were restricting outward transfers on 29 August 2025 and this must have been triggered for good reason.

The Arbiter considers it quite irrelevant whether contact started late August or early October as long as the transactions had already happened by 21 August 2025.

In any event, as Foris had transferred the assets to his Exchange account with a related company over which the Arbiter has no jurisdiction, as it is not registered or licensed in Malta, such questions should be more suitably addressed to Foris DAX Ltd, holder of the Exchange Account, that had received the assets by 21 August 2025. In fact, it has been confirmed that the warning of 29 August 2025 was issued by Foris DAX Ltd related to his exchange account.

[17] P. 80
[18] P. 79
[19] P. 80
[20] *Ibid.*

All considered, the Arbiter concludes that the outward transfers, if not personally authorised by the Complainant, were effected by the fraudsters through the gross negligence of the Complainant. Foris cannot be held responsible for his gross negligence. From Foris's point of view, the transfers were properly authorised by the Complainant through use of his secret access credentials.

The Arbiter also considered whether there is any responsibility on the part of the Service Provider in view of the fact that these payments were effected in 2025 when a service provider licensed under the VFA Act/MiCA regulatory regime (Regulation on markets in crypto assets EU 2023/1114) started being subject to the obligations of the Travel Rule under the TFR Recast.[21]

The TFR recast introduced **enhanced anti-money laundering (AML) and counter-terrorist financing (CTF) requirements** for **crypto-asset service providers** operating within the European Union. The regulation aims to *inter alia* improve the **traceability of transfers of funds and crypto-assets** and reduce financial crime.

One of the aspects considered is the impact of the Travel Rule, as a measure to protect against money laundering and the financing of terrorism, and the protection offered to the consumer who fell victim to fraud, which fraud could have been avoided if the CASP had honoured its obligation under the Travel Rule properly.

However, the Arbiter notes that the Travel Rule Guidelines are applicable to transfers of digital assets to external non-hosted wallets which the transferor declares as being under his control or ownership.

In this case, the transfers were effected to a hosted wallet, beneficially owned by the Complainant, with a related crypto exchange company. Accordingly, the procedures required under the Travel Rule guidance are not applicable.

[21] The Service Provider's VFA licence was surrendered on 27 January 2025, with the MiCA licence issued on the same day.

Decision

It is probable 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.

The Arbiter notes that the crypto business is a relatively new area. An EU regulatory framework was only recently implemented effective for the first time in this field in 2025.[22]

Whilst this area of business had remained 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.[23]

The Arbiter sympathises with the Complainant for the ordeal he may have suffered as a victim of a scam but, in the particular circumstances of this case, he cannot accept the Complainant's request for compensation as he has failed to provide any evidence of any regulatory breaches on the part of the Service Provider which contributed to the loss incurred.

[22] 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 entered into force in 2025 – https://www.financemagnates.com/cryptocurrency/can-mica-take-europe-to-the-crypto-promised-land/

[23] 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

For the above reasons, this complaint is not upheld and no compensation is being ordered.

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

Alfred Mifsud
Arbiter for Financial Services

<u>Information Note related to the Arbiter's decision</u>

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. Personal details of the Complainant(s) will be anonymised in terms of article 11(1)(f) of the Act.