Before the Arbiter for Financial Services

Case ASF 080/2025

QU

('the Complainant')

vs

Foris DAX MT Limited

(Reg. No. C88392)

('Foris' or 'Service Provider')

Sitting of 13 March 2026

The Arbiter,

Having seen the Complaint made against Foris DAX MT Limited relating to an unauthorised transfer of BTC (Bitcoin) 0.0266746 for a value of approximately €2,000 from his wallet with Crytpo.com (brand name of Service Provider)

The Complaint[1]

In his complaint form to the Office of the Arbiter for Financial Services ('OAFS'), the Complainant submitted that on 07 April 2025, he detected the unauthorised transfer on his wallet, and it resulted that his account was accessed without his consent from somebody with geographic location in Sweden whilst he was residing and operating exclusively from Spain.

He stated:

'*Even though I had correctly activated all available security measures (such as passcode and two-factor authentication), Crypto.com claimed that no changes*

[1] P. 1 - 7 with supporting documentation on P. 8 - 42.

to my device or login failures were detected, and therefore they do not consider it a case of account compromise attributable to their responsibility.

However, the evidence clearly shows a login from an unusual location (Sweden), which I reported immediately. Moreover, I always maintained control over my devices and never shared my credentials. Despite this, a significant transfer of funds was accessed and authorised. This contradiction between the platform's internal records and the facts I demonstrate has not been adequately considered.'[2]

He claims that the Service Provider refused to investigate the suspicious activity and refused to refund the loss caused by the transfer which he did not properly authorise.

By way of resolution, he is seeking full compensation for his loss amounting to about €2,000 and for Service Provider to take full responsibility for failure of their security protocols.[3]

Service Provider's reply

Having considered in its entirety, the Service Provider's reply[4] where they confirm that Complainant had been their client since 03 January 2021.

They confirmed that Complainant approached them on 07 April 2025 about a transfer subject of this complaint which was executed the day before at 22:16:06 hours. Upon such report, the wallet was temporarily disabled pending investigations.

Complainant was asked to complete a questionnaire regarding a suspected 'Account Takeover' (a scenario where scammers somehow manage to use the secret access credentials known only to the client to make unauthorised transactions which from the perspective of the Service Provider would appear properly authorised). This was immediately completed and returned by the Complainant.[5] It is noted that question 3.b, 3.c, and 4 were not replied to.

[2] P. 3
[3] P. 4
[4] P. 49 - 53 with attachments from p. 54 - 64
[5] P. 58 - 59; p. 61

Following further investigation, Complainant's request was declined as it resulted the transfer in question was properly authorised by Complainant and they stated:

'*Your wallet shows no registered change of access credentials, including no change of registered email address or passcode, before or at the time of the reported transactions.*

At the time of the incident, your account was accessed with your personal wallet credentials and the reported transaction(s) was/were initiated during the same session.

As outlined in our T&Cs that you agreed upon when opening your wallet, it is the account holder's responsibility to secure and protect their wallet account.

Conclusively, the reported events are not covered by the Account Protection Programme (APP) and/or the claim does not meet the minimum conditions for a relief by the APP.

For more information on the APP policy please visit Crypto.com APP Policy/Crypto.com Help Center.

Crypto.com cannot be held liable for any events or losses arising from the account holder's actions or inactions that lead to their account being compromised.

To ensure that you protect your account in the future we highly recommend that you take actions to secure your mobile device, personal email and Crypto.com wallet credentials.

Enabling the Crypto.com app security features is recommended at all times:

Multi-Factor Authentication (MFA) for all types of Transaction for which MFA is available.

Anti-Phishing Code (which identifies whether emails appearing to be form us are genuine).

24-Hour Withdrawal Lock for newly whitelisted addresses.

Also, consider enabling 2FA on your email account and be vigilant when clicking on URLs that may resemble Crypto.com's website or App.

While we understand that this may not be the response that you expected, we hope you understand that we are unable to refund or reverse the reported transactions.

Please consider referring the matter to your local police department as they may be able to help you retrieve your funds. Crypto.com will fully cooperate with any official police enquiries received to this regard.'[6]

Hearings

The Complainant failed to make presence for the first hearing scheduled for 16 September 2025.[7]

At a second hearing held on 04 December 2025, the Complainant confirmed all the evidence included in his complaint and had nothing further to add.

On being cross-examined he stated:

'Reference is made to page 10 of my complaint, whereby I state that I have done the multi-authentication processes for each transaction. Asked whether I enabled the multi-factor authentication for each transaction, I say that I did not authorise anything. I'm not sure if this is the question.

Asked whether I had the authentication factors, I say, yes, everything.

Asked whether I remember my phone being hacked at the time, I say, no.

Asked whether it was acting strangely or whether my account was hacked at the time, I say, nothing, nothing.

Asked whether I had the anti-phishing code on, I say, no, because I've never had any trouble and I did not need it. And I thought that the Crypto.com application was secure. Now, I am worried about it because I have everything in it. I have all my passwords. I never had anything strange on my account until that day.

[6] P. 51 - 52
[7] P. 71

Asked maybe I keep my passcode accessible to third parties on a notepad, I say, I always insert the passcode by hand, it is not in my phone.

Yeah, I always write it with hand, you say, not on my phone, in my house. Nobody can access my passwords.

Asked whether I live alone and whether no one comes to my house, I say that I live with my mother and my sister, but they don't even know I'm on the Crypto app.

Asked whether I remember receiving an e-mail notification on the 6th of April, prior to the transaction, requesting authorisation for login from a new device, I say no. I will screenshot everything, and that's not possible.

No, I do not remember receiving an email on 6 April. I received nothing. I did not receive this.

I am referred to the email sent by Crypto (page 41 of the complaint).

Asked whether I enabled the 24-hour withdrawal lock for newly whitelisted addresses as suggested by Crypto, I say, I do not remember. Maybe, yes, because the day I spoke with the Crypto.com service, I told them everything that had happened and they told me to activate something. Sorry, I don't remember.

Asked whether I filed a police report about the scam, about this unauthorised access, I say, no. I did not file a report with the police because I thought it was going to be useless.

Asked whether I am saying that my account was basically hacked, I say, yes.

Asked whether I saved the passwords or the codes that were received anywhere else apart from in my property, I say, no.

So, it is being said that I do not remember receiving an email notification requesting login from another device that I have.

I say that I did not receive anything strange before that day.

It is said that it was nothing strange but an email from Crypto requesting me to authorise for a login from a different device.

I say, no.

The Arbiter would like to have more clarification.

He states that according to the reply of Foris DAX MT, at the hour of 22:16:06, this transaction, which is claimed not authorised, had been effected. Obviously, for this transaction to be effected to a new wallet, it is obvious that the security precautions, for example, that a new wallet, once it is approved, would be locked for 24 hours, were not effected.

So, the Arbiter understands that when I complained then to Crypto.com and when I made the inquiries, they must have indicated to me what these security measures are. And I probably implemented these security commands. But then there is an email, which I sent with my complaint, (page 29) which shows that on the 7th of April-- so it's the next day after the payment was made-- at the hour of 18:40, the lock feature of the 24-hour withdrawal lock feature for new whitelisted addresses was disabled.

Asked whether I actually enabled this whitelisting after the payment was made and then I disabled it in the evening, I say, no.

The Arbiter states that I received this email from Crypto.com on Monday, 7th April at 20:40, saying that I disabled this feature at 18:40. So, the email was sent two hours after I disabled.

The Arbiter states that I received this email because I included it in my complaint; it is attached to my complaint, page 29 of the complaint.

I say that when I reported what happened, they told me that I have added to a whitelist the receiver, I mean the other address. So, my account does not need to be blocked. Does this make any sense?

The Arbiter explains that this happened on the 6th of April at 22:16. And for this thing to have happened on that day, at that hour, the recipient wallet must have been whitelisted by somebody. The Arbiter continues to explain that there is a security feature which says that when you adopt the security feature, when you whitelist a new address, you cannot make payments immediately, but you have to wait for 24 hours. And the security feature is there to protect against fraud. The fact that this was made, it appears to the Arbiter that I did not enable this security feature. But then, there is this email which the Arbiter

is referring to. which states that this security feature was disabled on the next day at 18:40 hours.

So, the Arbiter is of the understanding that between the payment which was made and this email, I had enabled the security feature and then, disabled it.

Asked whether this is so, I say that I did not disable anything.

The Arbiter asks me since I did not disable anything, what did I do when I received this email from Crypto.com on 7 April at 20:40, saying that since I disabled the 24-hour withdrawal lock for newly whitelisted addresses, this change will only take effect in 24 hours to save my funds.

Asked whether I did nothing, I say that I always spoke with the Crypto.com people from April. I do not know; I do not remember exactly what I did. I am sorry I cannot be more precise.

Everything I did. It's documented. I write everything'.[8]

At the third hearing on 12 January 2026. the Service Provider, through Pema Fung, stated:

'The Complainant became a client and user of the Service Provider on the 3rd of January 2021. The disputed transaction in question relates to one withdrawal of Bitcoin from the Complainant's Crypto.com account to one single external wallet address on the 6th of April 2024 at 22:16 UTC, which is Coordinated Universal Time.

This wallet address is what we call a non-custodial address, meaning they are not serviced by Crypto.com or identified on the blockchain as serviced by a similar Service Provider such as us. As part of the withdrawal process, as the withdrawal was made to a new wallet, this wallet address needed to pass through the whitelisting process. Firstly, the user would have had to complete the Travel Rule form, which he was asked to indicate whether the external wallet to which funds were being transferred was self-hosted or otherwise, and to specify the beneficiary of the external wallet.

As the crypto asset Service Provider of the originator, Foris DAX MT, obtained and maintained the information required under the Travel Rule regulation.

[8] P. 73 - 75

This included the name of the beneficiary, the beneficiary's distributed ledger address, and the unique transaction identifier of the external wallet.

Each transfer initiated by a user can therefore be individually identified. In this particular case, the transferor had indicated that the wallet was self-hosted, owned and controlled by themselves, and this was confirmed via a form submitted by them. This Travel Rule form was drafted by our internal compliance team and is considered to be compliant with the Travel Rule.

The Service Provider would also like to highlight the following points, which will be supplemented by screenshots that Dr. Bencini will then send to Mr. Arbiter and [Complainant].

The Complainant's log of account changes shows that the account was accessed from a new device with the Complainant's login credentials. The person who accessed the Complainant's account would have had to have access to his Crypto.com password and email address to authorise a login. There is no record of any change of password or email address at the material time. This is not the first time the Complainant has logged in with other devices, so it would not have raised any necessary flags.

For example, on the 13th of February, 2025, and on the 11th of March, 2023, logins from new devices were also identified in the log. At the material time, the Complainant had not enabled the anti-phishing email code. At the material time, the Complainant did not use the 24-hour withdrawal log. Had this feature been in place, the user would have had to wait 24 hours to make the withdrawal to the newly whitelisted withdrawal wallet address.

From a screenshot we can later show of the Complainant's user panel, we can see that the Complainant himself activated the 24-hour lock the day after the withdrawal and then disabled it some 24 hours after that. These were activated by the Complainant himself and can be shown because the email address that will be shown in one of the columns is that of the Complainant's newly changed email address after the alleged incident occurred.

As explained to the Complainant and as outlined in our terms and conditions, the Complainant is responsible for securing and protecting their account, including passwords and their email addresses.

Lastly, under the terms and conditions regarding our Account Protection Program, or APP as it's known, there are some minimum conditions to be met

before being eligible for APP relief, including, but not limited to, enabling an anti-phishing code in the Crypto.com app, which identifies whether emails appearing from us are genuine at least 21 days prior to the alleged unauthorised transactions, and enabling the 24-hour withdrawal lock for newly whitelisted addresses.

In this case, both of these conditions were not met. The transactions made appeared to us to have been made on a proper basis. Whoever made the transactions had access to the Complainant's passcode and registered email, and therefore the withdrawal appears to have been properly authorised. It is evident that to carry out this transaction in the undetected manner which the Complainant alleges, any third party would have had access to his email address.

On the balance of the foregoing, it is Foris DAX MT's case that the Complainant should be responsible for any losses which occurred out of his failure to carefully maintain the security of his account.

In summary, the Service Provider would submit that if an account takeover event had occurred, and the unauthorised transaction was not carried out by the Complainant, it was the direct result of either the negligence of the Complainant's part or willful or unwilful participation of the Complainant in the exposure of his personal credentials."[9]

No cross-examination was conducted by Complainant.

Following the hearing, the Service Provider submitted translated texts of several conversations held immediately between the parties following discovery of the contested payments[10] and evidence that the payment was approved by somebody who had the secret credentials to an address claimed as belonging to Complainant.[11]

One notes that in this exchange of chats Complainant admitted that:

'… the only thing I did that was out of the ordinary was give my BTC wallet to a guy to receive some income';[12]

[9] P. 76 - 78
[10] P. 86 - 111
[11] P. 85
[12] P. 88

'Recently, someone made a couple of transactions against me, one for around €300 and another for €600.'[13]

This contrasts with strong declarations in his complaint and evidence that nothing out of the ordinary was evident on his account with Crypto.com.

Service Provider also submitted logs showing changes made to access credentials over the period from initiation of the relationship to the time of the contested transfer.[14]

Final Submissions

In their final submissions, the parties merely restated their positions. Complainant continued to insist that he did not authorise the transaction. Service Provider affirmed that Complainant had not taken minimum precautions to protect his account so that the anti-phishing safety feature on the App and the 24-hour withdrawal lock for newly whitelisted addresses were not enabled at the time of the transfer in question.

Having heard the parties

Having seen all the documents

Considers

That the balance of probability is clearly on the side of the Service Provider given that:

1. There are glaring inconsistencies between what is stated in the chats recorded after the loss was reported and the strong assertions of the Complaint that he did not disclose to anyone his access credentials.
2. Important security features of the system were not activated as Complainant considered them optional.
3. Complainant admitted he gave his BTC wallet to an unknown person believing he would gain extra income.[15] It is untypically coincidental that his BTC units were taken from his Crypto wallet in what appeared to be

[13] P. 94
[14] P. 131 - 143
[15] P. 88

an authorised transaction without his having given not only his BTC wallet address but also his access credentials, knowingly or unknowingly.

4. Complainant admitted he had other strange transactions over his account before the reported 'incident' leading to the complaint.[16]

Consequently, 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

Information Note related to the Arbiter's decision

Right of Appeal

The Arbiter's Decision is legally binding on the parties, subject only to the right of an appeal regulated by article 27 of the Arbiter for Financial Services Act (Cap. 555) ('the Act') to the Court of Appeal (Inferior Jurisdiction), not later than twenty (20) days from the date of notification of the Decision or, in the event of a request for clarification or correction of the Decision requested in terms of article 26(4) of the Act, from the date of notification of such interpretation or clarification or correction as provided for under article 27(3) of the Act.

Any requests for clarification of the award or requests to correct any errors in computation or clerical or typographical or similar errors requested in terms of article 26(4) of the Act, are to be filed with the Arbiter, with a copy to the other party, within fifteen (15) days from notification of the Decision in terms of the said article.

[16] P. 94

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.