**Before the Arbiter for Financial Services**

**Case ASF 149/2021**

**NZ ('the Complainant')**

**vs**

**Foris DAX MT Limited (C 88392)**

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

**Sitting of the 28 September 2022**

**The Arbiter,**

Having seen **the Complaint** relating to the alleged unauthorised transactions undertaken from the Complainant's account held with *Crypto.com*, where her cryptocurrency holdings were transferred into other digital asset/s (crypto) and subsequently withdrawn to an external wallet address, resulting into her cryptocurrencies being purportedly stolen.

*The Complaint*

The Complainant explained that she was an investor on the Service Provider's platform and that an incident occurred in relation to her crypto coins.

She explained that her crypto coins were completely wiped out of her account. It was claimed that the issue was that there were several discrepancies in the descriptions provided by the Service Provider in trying to convince her as to the true nature of what had happened.

The Complainant further explained that she was new to crypto investment, but the Service Provider's platform made it easy to buy and hold cryptos. She started to slowly purchase and hold cryptos and had amassed about 22 million Shib coins,

5000 Doge coins and some other crypto. She noted that every purchase comes with an automatic email confirmation from the platform.

It was noted that on the night of 27/09/2021, the Complainant updated her iOS and after the update she tried to login on *Crypto.com* but her Face ID failed. She further noted that she then clicked on *'Forgot Pin'* and after managing to login into her account, she discovered that all her coins were gone.

The Complainant explained that she had been through an annoying rigorous check with the Service Provider who refused to return her coins and did not answer some pertinent questions such as the following:

- how her account was accessed as her phone had not been compromised in any way;
- how a transaction was made given her pin was not written anywhere and hence why she could not remember it and had to do a reset;
- how she did not receive any email confirmation/notification in respect of the transactions/withdrawals made.

The Complainant submitted that it was obvious that there was an internal issue with *Crypto.com* and that either the App had a security flaw, or it was hacked from a source/backend or someone from the Service Provider's team was stealing people's cryptocurrencies and passing it off as the client's fault, given that it made absolutely no sense.

The Complainant reiterated its belief that *Crypto.com* has a flaw or that they had been hacked or it was an internal or inside job.

She explained that, at first, she thought it was all just a simple misunderstanding and the matter should be rectified in a day or two, but she was dumbfounded with the result of the Service Provider's investigation which claimed that her phone was compromised. She questioned how this could have happened.

The Complainant submitted that the Service Provider did not do its due diligence and find where her crypto had been moved/transferred and who authorised it. Neither did the Service Provider consider why she did not receive an email confirmation for every single step of the conversion of each of her coins (Shiba Inu, Doge, CRO, COS), given that *Crypto.com* had sent email notification for every

process initiated from her account. She noted that, suddenly, on the day of the conversion and withdrawals, all crypto had miraculously disappeared with no single notification sent to her. She claimed that this was definitely fishy.

The Complainant submitted that the Service Provider is refusing to carry out a thorough investigation and has accused her of something which it clearly knows is not the Complainant's fault. The Complainant noted that this was her hard-earned money and should be protected. She claimed that the Service Provider has failed to protect her and her investment on a platform that they provided.

*Remedy requested*

The Complainant requested all her cryptocurrencies back and a maximum compensation for her mental health as she had been traumatised by such event and her entire family was put in a state of confusion and panic.

She noted that she had to be rushed to hospital twice over a panic attack out of fear that she had lost her entire investment.

The Complainant listed the following as her cryptocurrencies:[1]

- SHIBU 22,600,000
- Doge 3,500
- CRO 2,203
- Cos 1000

It was noted that she cannot ascertain the value of the coins currently, given that cryptos are extremely volatile as they rise and fall daily, and she did not want to speculate and mislead in any way or form.

**In its reply, Foris DAX MT Limited essentially submitted the following:**[2]

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.

[1] P. 4
[2] P. 109-112

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 via a mobile device.

That the Complainant became its customer through the *Crypto.com* App and was approved to use the Wallet on the 25 May 2020.

The following timeline was provided by the Service Provider:

a) 28 September 2021 – The Complainant contacted *Crypto.com* Customer Support reporting that the cryptocurrency assets within her *Crypto.com* Wallet were missing.

   It was noted that during the communication, the Complainant claimed that on 27 September 2021 her Wallet was accessed by a third party who exchanged three of her virtual asset holdings (CRO, SHB, USDT) into Dogecoin (DOGE). The total amount of 5,651.05040727 DOGE was then withdrawn to an external wallet address that the Complainant has no access to. A screenshot of the reported unauthorised activity was provided.[3]

   The Complainant's Wallet was temporarily disabled and upon authentication of her identity via a current selfie photograph, the reported case was escalated to Foris DAX Risk Team for a review. The case was then classified as an alleged account takeover ('ATO') and put through Foris Dax's ATO Internal Process. The Complainant was subsequently requested to reply to an 'Account Takeover Questionnaire'.

b) 29 September 2021 – The Complainant provided the completed Account Takeover Questionnaire.

c) 30 September 2021 – The assessment of the ATO case was completed by the Risk Team and their decision was provided to the Complainant via email.

   Following receipt of the ATO Questionnaire, the Risk Team reviewed the answers and issued an opinion that, based on the facts laid out in said questionnaire and the chain of events visible within their system, a reimbursement of the claimed amounts was to be declined due to a clear

[3] P. 110

indication that the Complainant had wilfully or unwilfully, by exerting negligence in regards to the privacy and security of her personal credentials, facilitated the alleged unauthorised access to her Wallet.

The Service Provider provided additional context in support of the said decision as follows:

- It noted that the alleged hacker must have been in possession of the Complainant's *Crypto.com* Wallet App passcode and must have had access to the Complainant's registered personal email in order to access the Wallet and execute the said transactions.

  Foris DAX audit trail showed that no change of passcode or login credentials, or any failed login attempts had been registered for the Complainant's Wallet and hence one can conclude that the Wallet had been accessed with the same credentials used before the date of the reported incident – the same email address and passcode.

- The login to the *Crypto.com* Wallet App from the new device was confirmed from the user's registered email address.

In its reply, the Service Provider provided a screenshot of the feedback sent to the Complainant. The said feedback read as follows:[4]

*'We have investigated your claim of unauthorised activities and crypto withdrawal.*

*The outcome of our investigation is that we did not find any abnormalities since there was no change of the email used to access your account, which means that whoever accessed your account had access to your email client prior to initiating any transactions or updates.*

*We highly recommend that you take action to protect your mobile device, email and Crypto.com wallet details – specifically and especially the pass-code – along with any personal data stored in your device.*

[4] P. 111

> *Also please consider enabling our additional security features – the 2FA setup and the Anti-phishing Code. You can find those features in your Crypto.com App Settings panel.*
>
> *As outlined in our T&Cs and further acknowledged by you, it is the account holder's responsibility to secure and protect their wallet account. In accordance with the Payment Service Directive (PSD2), Crypto.com cannot be held liable in cases of gross negligence'.*

The Service Provider submitted that, contrary to the claim made by the Complainant that Foris DAX has not sent email notifications regarding the reported unauthorised transactions dated 27 September, they had records to prove that its system had successfully sent emails confirming each individual transaction. A screenshot was provided in its reply of the confirmations from its back office.[5]

The Service Provider further submitted that, in summary, it considers that the Account Takeover to be the result of either (i) negligence on the Complainant's part or (ii) wilful or unwilful participation of the Complainant in the exposure of her personal credentials.

To successfully carry out the unauthorised activity, the alleged perpetrator had to be in possession of (i) the Complainant's Wallet passcode and (ii) have access to the Complainant's personal email. Both items are accessible by the use of personal credentials (or via saved logins on a personal device owned by the Complainant) that are in the sole possession of the Complainant.

The Service Provider further noted that it is unable to reverse any of the transactions performed through the Complainant's Wallet since transactions done on the blockchain are immediate and immutable.

**Preliminary**

*Nature of Complaint and allegations*

The Arbiter notes that in her complaint to the Office of the Arbiter for Financial Services, the Complainant claimed that the loss of all her cryptocurrencies held

[5] P. 111

with *Crypto.com*, which were withdrawn to an external wallet by an alleged unauthorised party, was *'an internal issue with crypto.com'*.[6]

In her Complaint, she further made the claim against Foris DAX, that *'it's either your App has a security flaw or it has been hacked from source/backend or someone in your team is stealing peoples cryptocurrencies and passing it off as clients fault'*.[7]

She subsequently complained that Foris DAX *'refuse to carry out [a] thorough investigation'* and *'failed to protect [her] and [her] investment on a platform they provided'*.[8]

The Arbiter also notes that in the numerous chats the Complainant exchanged with Foris DAX, a copy of which were attached to her Complaint,[9] the Complainant made the serious accusation that Foris DAX had a *'fraudulent platform'*,[10] claiming that *'someone in your company stole my money'* and that she considered this as *'an inside job'*.[11]

**The Arbiter would like to outrightly emphasise that allegations of criminal fraud are not handled by the Office of the Arbiter for Financial Services. Such type of allegations is a matter for the police to handle. Any allegations of criminal fraud should accordingly be reported to the police and relevant authorities.**

**In this Complaint, the Arbiter shall accordingly not review or consider any allegations of fraud but will only focus and consider those matters which fall within his powers under the Arbiter for Financial Services Act (Cap. 555).**

**The matters that will be considered by the Arbiter are therefore the following:**

**(i) The Complainant's claim that Foris DAX refused to carry out a thorough investigation of the events that led to her alleged theft of the cryptocurrencies from her account held with *Crypto.com*;**

[6] P. 3
[7] *Ibid.*
[8] P. 4
[9] The Complainant produced nearly 70 pages of messages exchanged between her and the Support Team of *Crypto.com* (P. 36 - 103)
[10] P. 52 & 57
[11] P. 78

**(ii) The Complainant's claim that Foris DAX failed to protect her *Crypto.com* account and the cryptocurrencies held within the said account.**

**The said claims will be considered taking into consideration the pertinent aspects, including the relevant submissions made by the Complainant and the obligations that Foris DAX was subject to in terms of the applicable regulatory framework and the terms and conditions in respect of the service provided, as applicable at the time.**

**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[12] which stipulates that he should deal with complaints in '*an economical and expeditious manner'.*

*The Complainant and her crypto account*

The Service Provider stated that the Complainant became a customer of Foris DAX on 25 May 2020 upon signing up for the *Crypto.com App*.[13]

In the chat communications that the Complainant exchanged with the technical support staff of *Crypto.com*, the Complainant, who is resident in London,[14] described herself as a *'a single mother with 3 children'* [15] who worked as a cleaner.[16]

[12] Art. 19(3)(d)
[13] P. 109 & 158
[14] P. 1
[15] P. 57
[16] P. 40

In the said communications, she had also remarked that *'someday [she] had no food but kept invest[ing so] that one day, [she] can reach [her] goals'* but now had *'all [her] savings gone'*. [17]

Her experience with cryptocurrencies seems limited given that, as noted in her chat communications, she did not *'even know how to use the app fully'*, as *'this is my first ever crypto app'*.[18]

In her Complaint, the Complainant indicated that she had the following cryptocurrencies:[19]

- 22,600,000 SHIB
- 3,500 DOGE
- 2,203 CRO
- 1,000 Cos

She claimed that she *'never made any withdrawals'* from her account and the only transactions undertaken just consisted of purchases of cryptocurrencies.[20]

As per the transaction overview statement produced by the Service Provider and the information provided during the proceedings of the case, the following transactions occurred on the Complainant's account on 27 September 2021:[21]

- Exchange of 2000 CRO
- Exchange of 7,000,000 SHIB
- Exchange of another 15,600,000 SHIB
- Exchange of 466.188434 USDT
- Withdrawal of 3192.95040727 DOGE
- Withdrawal of 2558.1 DOGE

[17] P. 40
[18] P. 99 & 103
[19] P. 4
[20] P. 99 & 103
[21] P. 66, 110 & 156

Whilst the total amount of 22,600,000 SHIB above reflects the amount of crypto indicated by the Complainant in her Complaint as forming part of her portfolio, the Arbiter could not reconcile exactly the amounts of the CRO and COS crypto indicated by the Complainant with the list of withdrawn currencies.[22]

The total amount of 5,751.05040727 DOGE were withdrawn to an external wallet. During the hearing of 29 March 2022, the Service Provider testified that the *'actual value at the time the transactions happened is around €1,000'*, these being the liquidated proceeds.[23]

*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.[24]

Foris DAX is licensed by the Malta Financial Services Authority ('MFSA') as a VFA Service Provider as per the MFSA's Financial Services Register.[25] 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.[26]

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'*.[27]

---

[22] The transactions listed by the Service Provider as being exchanged and eventually withdrawn only indicate 2,000 CRO (203 CRO in less than the figure indicated by the Complainant) and no COS. The 3,500 DOGE indicated by the Complainant seems to form part of the 5,751 DOGE withdrawn to the external wallet - i.e. 3,500 + 2,251 DOGE. As per the extracts from the communications exchanged between the Complainant and the Support Team of *Crypto.com*, the CRO and SHIB currencies appear to have been first exchanged into USDT and then the amount in USDT exchanged for 2,251.10 DOGE (P.66 & 67).

[23] P. 158

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

[25] https://www.mfsa.mt/financial-services-register/

[26] https://www.mfsa.mt/financial-services-register/

[27] 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 ...'*.[28]

It offers the account holder *'a crypto custodial wallet'* and *'the purchase and sale of digital assets on own account'*.[29]

***Observations & Conclusion***

*Summary of main aspects*

The Complainant claimed that someone had stolen her cryptocurrencies from her *Crypto.com* account. She claimed that there were unauthorised transactions resulting in her cryptocurrencies being completely wiped out from her account.[30]

As testified during the hearing of 15 March 2022, the Complainant tried to log into the *Crypto.com* app but could not do so at the time when her crypto were stolen.[31] She discovered that her cryptocurrencies were gone after being given back access to her account following the verification process she had to do with the Service Provider to regain access.[32]

As indicated by the Service Provider, the Complainant contacted Foris DAX within a day, on the 28 September 2021,[33] with the difficulties she was experiencing on her account, but this was nevertheless too late as her crypto wallet had already been emptied by then.

The Complainant strongly denied that she initiated any withdrawals herself and also denied she received any confirmations in her mailbox of the withdrawals undertaken from her account. She claimed that she had never withdrawn any cryptocurrencies from her account with her transactions only consisting of just purchases of crypto.

[28] P. 131
[29] P. 109
[30] P. 36
[31] P. 127
[32] *Ibid.*
[33] From the disputed transactions undertaken on 27 September 2021

In this investigation of the events that led to her alleged theft of cryptocurrencies from her *Crypto.com* account and whether Foris DAX failed to protect her *Crypto.com* account and part of the decision, the Arbiter shall consider the two main aspects of the Complainant's allegations, namely, whether Foris DAX refused to carry out a thorough crypto portfolio.

*Applicable Regulatory Framework*

As outlined above, Foris DAX is the holder of a Class 3 VFAA licence granted under the Virtual Financial Assets Act, 2018 ('VFAA').

By virtue of its licence under the VFAA, the Service Provider is obliged to have in place *'adequate internal control or security mechanism'*, where these are to be *'comprehensive and proportionate to the nature, scale and complexity of the VFA services to be provided'*.[34]

In terms of Article 23(2) of the VFAA, which relates to *'Applicable requirements and compliance with the Prevention of Money Laundering Act*', the Service Provider is further required to *'ensure that all of its systems and security access protocols are maintained at all times to appropriate high standards'*.

It is noted that Article 38(1)(e) of the VFAA, which relates to the *'Minister's power to make regulations'*, provides for the enactment of regulations to *'define the criteria for determining whether the systems and security access protocols of issuers, applicants or licence holders, as applicable, meet or are maintained to the appropriate high international standards that may be established from time to time'*.

The regulations so far issued in terms of the powers conferred by article 38 of the VFAA are the *Virtual Financial Assets Regulations, 2018 (L.N. 357 of 2018)*. The said regulations namely deal with exemptions from requirements under the VFAA, the payment of licence fees, requirements relating to control of assets and clients' money as a distinct patrimony apart from administrative penalties and appeals. **Such regulations do not include criteria relating to the systems and security access protocols as referred to under article 38(1)(e) mentioned above.**

[34] Example – As per Article 17(e) of the VFAA which deals with *'Where the competent authority shall refuse to grant a licence'*.

It is further noted that the MFSA has issued a rulebook, the *Virtual Financial Assets Rulebook ('the VFA Rulebook')* which complements the VFAA by detailing *inter alia* ongoing obligations applicable for VFA Service Providers.

Chapter 3 of the VFA Rulebook includes the rules applicable for VFA Service Providers which such providers must adhere to.

Title 1, Section 2 of Chapter 3 of the said VFA Rulebook details a number of High-Level Principles. Such principles include Rule *R3-1.2.1*, which requires that:

*'VFA Service Providers shall act in an ethical manner taking into consideration the best interests of their clients and the integrity of Malta's financial system'*.

Furthermore, Rule *R3-1.2.4(i)* provides that:

*'In complying with R3-1.2.1, VFA Service Providers and their related Functionaries shall: i. make reference to, and where applicable comply with, the applicable Maltese laws, VFA Regulations and the Rules issued thereunder as well as any Guidance Notes which may be issued by the MFSA or other relevant body to assist the said persons in complying with their legal and regulatory obligations'*.

Chapter 3 of the VFA Rulebook also details various requirements that must be satisfied by a VFA Service Provider with respect to the security of its systems. For example, Rule *R3-3.1.2.1.3(iii)* of *'Title 3, Ongoing Obligations for VFA Service Providers', Chapter 3 of the VFA Rulebook,* requires that:

'*The Licence Holder shall: ... iii. establish, implement and maintain adequate internal control mechanisms designed to secure compliance with decisions and procedures at all levels of the Licence Holder',* where *'the Licence Holder shall take into account the nature, scale and complexity of its business, and the nature and range of VFA services undertaken in the course of that business'*.

In turn, Rule *R3-3.1.2.1.4* requires that:

*'The Licence Holder shall ensure that it has sound administrative and accounting procedures, internal control mechanisms, effective procedures for risk assessment, and effective control and safeguard arrangements for information processing systems',*

whilst, Rule *R3-3.1.2.1.5* (i)&(vi) details that:

*'Without prejudice to R3-3.1.2.1.4, the Licence Holder shall establish, implement and maintain:*

*i. systems and procedures that are adequate to safeguard the security, integrity and confidentiality of information, taking into account the nature of the information in question;*

*...*

*vi. adequate security arrangements including inter alia in relation to cyber security'.*

It is further noted that with respect to security measures, Rule *R3-3.1.2.1.6* stipulates that:

*'The Licence Holder shall have sound security mechanisms in place to guarantee the security and authentication of the means of transfer of information, minimise the risk of data corruption and unauthorised access and to prevent information leakage maintaining confidentiality of data at all times.'*

Rule *R3-3.1.2.1.8* of the said part of the VFA Rulebook further specifies that:

*'Notwithstanding point (vi) of R3-3.1.2.1.5 and R3-3.1.2.1.6, a Licence Holder shall ensure that its cybersecurity architecture complies with any internationally and nationally recognised cyber security standards, any guidelines issued by the Authority and shall also be in line with the provisions of the GDPR.*

*Provided that for purposes of this rule, the Licence Holder shall take into account the nature, scale and complexity of its business.'*

It is further noted that Rule R3-3.1.2.2.8 (vii) details that:

*'the Board of Administration shall ensure adequate systems and controls from an Information Technology point of view, including inter alia with respect to cyber-security.'*

Rule *R3-3.1.5.4.3* in turn specifies that:

*'Where the business model of the Licence Holder involves the custody of Assets - party Custodian, the said Licence Holder shall ensure that such service is provided in line with internationally and nationally recognised best practices and cyber security standards, as well as any guidelines issued by the Authority.'*

The Service Provider has also the obligation to monitor and evaluate its systems and controls as per *Rule, R3-3.1.2.1.7* which requires the following:

*'The Licence Holder shall monitor and, on a regular basis evaluate, the adequacy and effectiveness of its systems, internal control mechanisms and arrangements established in accordance with R3-3.1.2.1.1 and R3-3.1.2.1.3 and take appropriate measures to address any deficiencies'.*

The Arbiter further notes that in the year 2020, the MFSA has also issued a *'harmonised baseline guidance on Technology Arrangements'*[35] 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').

It is particularly noted that Guidance 4.7.7(g) which relates to User Authentication Methods, specifies the following:

*' 4.7.7 Licence Holders should define, document and implement procedures for logical access control (identity and access management). These procedures should be implemented, enforced, monitored and periodically reviewed. The procedures should also include controls for monitoring anomalies, and should, at a minimum, implement the following:*

...

*i) User authentication methods: Licence Holders should enforce authentication methods that are sufficiently robust to adequately and effectively ensure that access control policies and procedures are complied with. Authentication methods should be commensurate with the criticality of ICT systems, the information or the process being accessed. This should as a minimum strong passwords or stronger authentication methods based on relevant risk (e.g.*

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

*two-factor or multi-factor authentication for access that is fraud sensitive, allows access to highly confidential/sensitive information, or that could have material consequences for critical operations). Licence Holders subject to Directive (EU) 2015/2366 (PSD2) should ensure compliance with Regulatory Technical Standards (RTS) on Strong Customer Authentication (SCA) and common and secure open standards of communication'*

***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 for the reimbursement by the Service Provider of the sum allegedly stolen from her crypto account**.

This is when taking into consideration various factors and for the reasons outlined below.

(i) *Allegation that Foris DAX refused to carry out a thorough investigation*

**The Arbiter considers that there is no satisfactory and sufficient evidence that the Service Provider failed to thoroughly investigate the Complainant's case, also, in light of the several communications exchanged between the Complainant and the Service Provider, and the feedback emerging from the said multiple communications.**[36]

(ii) *Allegation that Foris DAX failed to protect her account and crypto*

**Taking into consideration the nature of the complaint, activities involved, the alleged shortfalls as well as other pertinent aspects as outlined below, the Arbiter considers that there is no adequate and sufficient basis either substantiating the Complainant's claim that the Service Provider failed to protect her account and portfolio of cryptocurrencies.**

- *Nature of complaint, activities involved and alleged shortfalls*

[36] Such as the email of 30 September 2021 (P. 111) and extracts of the chats with the Customer Support Team of *Crypto.com* (P.36-103) and (P.113-126).

**As to the reasons why the Complainant deemed Foris DAX as having failed to protect her crypto account and assets, it is noted that in her final submissions, the Complainant stated that she never sold, transferred or exchanged her cryptocurrencies within the *Crypto.com app* and only used the app to purchase and accumulate crypto within her account. Hence, it was implicitly argued that it was abnormal that all of a sudden someone had initiated a transaction that did not involve a purchase but rather the exchange of coins and transfer to an external wallet.**

**The exchange of coins and/or transfers to external wallets are however, in their own right, not considered as something abnormal in the crypto field given that such exchanges and transfers are features commonly available in a customer's crypto account.**

**The Complainant also pointed out that a *'NEW device that is not registered to their network'* was used and *'an alarm did not go off'*.[37]**

**She stated that:**

***'Crypto.com claimed an email was sent to me which I never received they also claim my crypto.com app was comprised which is also impossible because my iPhone use facial ID'*.[38]**

**The Complainant emphasised that she never received any notifications by email. She claimed that she did not receive the *'Magic Link'* (i.e. the notification/validation request by email of the new device) which the Service Provider claimed was sent to her email address. She also stated that she did not receive any notifications by email of the transactions (i.e., exchange/transfers) undertaken from her account.**

**Whilst the claims made by the parties could not be verified and/or were not satisfactorily substantiated during the case, however, the explanations provided by the Service Provider during the hearing of 29 March 2022, on the use of the new device and notification of trades, are**

[37] P. 163
[38] *Ibid*.

**considered by the Arbiter to be more plausible. The said explanations also do not give rise to any evident material shortfall.[39]**

**In case where the Complainant's email was compromised, which seems to be the case, someone would have had access to her email from devices other than her mobile phone. The Complainant has not indicated that she had any additional security features (like 2 Factor Authentication) on her email account either. 2 FA is a common security option available also for email accounts that provides an extra layer of security to access one's email account.**

**In her final submissions, the Complainant indicated that she contacted *'Yahoo.com about my email been compromised and they said in clear terms no such things took place'*.[40] No evidence was however provided of such alleged communication and confirmation by the email provider.**

**As to the access to the *Crypto.com App*, the Arbiter further notes that, as indicated in the Service Provider's email to the Complainant of the 30 September 2021, Foris DAX had in place *'additional security features – the 2FA setup and Anti-phishing Code'* where such features, (which the Complainant could have availed of), could be found in the *'Crypto.com App Settings panel'*.[41] It is clear that this would have made the access to the *Crypto.com* account more secure. Unfortunately, for some reason, these were not implemented by the Complainant.**

**Whilst the Complainant was not aware of, nor did she indicate, any instances where her login details for the *Crypto.com* App as well as her email account could have possibly got compromised, the case in question has all the features of an Account Takeover where a third party got access to the Complainant's login details of her email account and *Crypto.com* account.**

**Sadly, there are various common cryptocurrency scams, such as '*Phishing Scams'* and *'Social Media Cryptocurrency Giveaway Scams'***

[39] P. 158-162
[40] P. 163
[41] P. 111

**which are used by scammers to obtain the customer's credentials through malicious links and fake websites.[42] It looks likely that the Complainant had unfortunately fallen victim for such a scam without possibly realising.**

**On the basis of the facts the Arbiter had before him, he 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.**

**Furthermore, the Complainant only noted, in her final submissions, that:**

***'Crypto.com is a financial institution should be treated as such and all obligations and responsibilities accorded to such organisations should be accorded to them'*.[43]**

**She further noted that *'Crypto.com are currently issuing Visa cards of different grades they ultimately a financial institution and must be treated as such...'*.[44]**

**The Arbiter would like to point out, however, that Foris DAX is not a regulated financial institution but is only regulated and licensed as a VFA Service Provider as outlined above. The regulatory regime applicable to a VFA Service Provider is indeed a different one and does not necessarily reflect the requirements and consumer protection measures applicable to a financial institution falling under EU regulatory regimes.[45]**

**The entity which has a financial institution license in terms of the Financial Institutions Act is Foris MT Limited (this being a distinct group entity) and it is this entity and the activities provided by such which is subject to the provisions of the Payments Services Directive. The**

[42] https://www.techtarget.com/whatis/feature/Common-cryptocurrency-scams
[43] P. 163
[44] P. 164
[45] 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).

**Complainant was not a customer of Foris MT Limited but of Foris DAX where the nature of the activities provided are different.**

**The Arbiter further 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 indeed still yet to be implemented for the first time in this field within the EU.[46]**

**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 home-grown national regulatory regimes. However, such regimes, which 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.**

**Indeed, 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.[47]**

- *Lack of satisfactory evidence on key aspects*

**Whilst there is no reason to doubt the Complainant's claim that her crypto assets have been stolen by a third party, such a claim is however difficult to verify and corroborate to a satisfactory level**.

[46] 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 2023 / 2024 – https://www.financemagnates.com/cryptocurrency/can-mica-take-europe-to-the-crypto-promised-land/

[47] 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

**As outlined above, the Complainant's case is further weakened when no satisfactory evidence 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 contractual and/or arising from the regulatory regime applicable at the time of the disputed transactions in respect of the services provided.**

- *Absence of legal provisions and regulatory requirements involving Strong Customer Authentication and refunds in case of unauthorised transactions*

**It has not emerged that the local regulatory regime applicable to the Service Provider imposed a mandatory requirement for the application of Strong Customer Authentication[48] to access an account.**

**In the circumstances, the Arbiter cannot accordingly determine either that the Complainant had, at the time, a reasonable and legitimate expectation for the Service Provider to mandatorily apply a higher level of security such as two-factor authentication, 2FA, to access her *Crypto.com* account, which would have reduced the risk of an account takeover.**

**Moreover, as indicated above, 2FA was available to the Complainant at the time of the disputed transactions but had not been availed of by the Complainant herself - either because she was not aware of such feature or because she consciously opted not to apply it**.[49]

**Lastly, the Arbiter notes that the regulatory framework specifically applicable to the Service Provider does not include either any provisions to cater for liability and eligibility of possible refunds in case of unauthorised transactions as, for example, found in other well-established sectors of the financial services industry**.[50]

[48] Such as that equivalent or similar to Strong Customer Authentication as defined under Directive (EU) 2015/2366 on payment services, the Payment Services Directive (PSD2)
[49] Email of 30 September 2021 of the Service Provider – P. 111
[50] Example - Articles 73 and 74 of the EU's Payment Services Directive (PSD 2), which apply to financial/payments institutions falling under the said Directive.

**Decision**

**The Arbiter sympathises with the Complainant for the ordeal she suffered due to the loss of her assets, but he cannot accept her request for compensation. For the reasons amply explained above, this Complaint is accordingly being rejected.**

However, since cryptocurrency 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, 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.

The Arbiter cannot help but notice the lack of, and inadequate education that many retail consumers have in this field, despite the rush by many to join and participate into this sector.

The Arbiter considers that much more needs to be done on this front, apart from in other areas, to better protect consumers. Genuine service providers operating in this field need to also do their part and actively work to improve the much-needed knowledge for consumers who opt to venture into this field.

**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**