Before the Arbiter for Financial Services

Case ASF 036/2022

GI

('the Complainant')

vs

Foris DAX MT Limited (C 56013)

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

Sitting of 8 May 2023

The Arbiter,

Having seen **the Complaint** relating to the alleged unauthorised access to and the subsequent transactions from the Complainant's account held with *Crypto.com*.

The Complainant explained that two transfers were made in the *Crypto.com* application and an NFT account was created in her name for the amount of $9,895 and another one for the amount of $9,454. She claimed to have communicated this with *Crypto.com* but was told that they have been able to recover only one part of such transfers and returned 0.19 Bitcoin.

The Complainant noted that the provider allowed transfers to be made without her consent, when knowing that the IP and location was not hers, and when even having the double authentication factor.

She insisted that, considering the matter is related to a security problem of the *Crypto.com* application, she expects the funds in question to be fully recovered. In fact, she is requesting[1] the provider to return the remaining funds that were

[1] P. 3

transferred from her account without her consent, that is, the remaining €10,000 or the 5 Ethereum that she had at that time.

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.

It is noted 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 an App on a mobile device ('the Crypto.com Wallet app'). On the other hand, the services of Crypto.com NFT Platform ('NFT Platform') together with separate NFT account ('NFT Account') for every customer registered on such platform are offered by Foris DAX Global limited, this being a company based in Ireland.

The Service Provider explained that the Complainant became its customer through the *Crypto.com* App on the 2 February 2021 and made use of the Wallet services offered by Foris DAX. She then became a customer of Foris DAX Global limited on 3 January 2022 through the Crypto.com NFT Platform Website and a subsequent holder of an NFT account.

The following timeline was provided by the Service Provider:

a) 3 January 2022 – The Crypto.com Risk team detected suspicious logins and transactions on the Complainant's Wallet. As a result, the Wallet was temporarily suspended so to prevent any damages.

b) 10 January 2022 – An internal escalation was opened in order to address what was considered to be a potential account takeover ('ATO'). The Crypto.com Customer Service Team was asked to contact the complainant, verify her identity as per the Service Provider's established process, gather information regarding the mobile devices that have access to her Wallet and confirm the latest transactional activity.

c) 12 January 2022 – The Complainant was contacted via email, by virtue of which, she was requested to confirm the model of the devices from which she can access her *Crypto.com* account, the name of the internet provider she uses to log in to her account, and the city of district from which she usually

[2] P. 37 - 43

accesses her account. For security reasons, further measures were required for the complainant to be authenticated prior to proceeding.

d) 9 February 2022 – The Complainant, who failed to reply to the provider's email communication, contacted *Crypto.com* Customer Support through the in-app chat facility reporting several unauthorized transactions. The provider noted that during the communication, the Complainant claimed that on 3 January 2022, her wallet was accessed by a third party who performed an unauthorised exchange of 873.40855074 of her Cronos (CRO) into 0.131482 ETH (Ethereum), and two unauthorized ETH (Ethereum) payments towards the *Crypto.com* NFT platform. A screenshot[3] from the provider's system of all the reported unauthorised activities was included as part of its reply.

   The Service Provider explained that upon authentication of the Complainant's identity, including a current selfie photographed by the Complainant to this effect, the reported case was escalated to the company's Risk Team for additional review.

   It further noted that the case was 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'.

e) 15 February 2022 – The Complainant provided the completed Account Takeover Questionnaire.

   Foris DAX noted that, based on the facts laid out in the said Questionnaire and chain of events visible on its system, the Risk Team issued an opinion that the Complainant had willfully or by exerting negligence in regard 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 perpetrator 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 above-mentioned transactions.

[3] P. 39

Foris DAX's audit trail showed no change of passcode or login credentials, neither any failed login attempts had been registered for the Complainant's Wallet prior to the execution of the said transactions 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 as provided and set by the Complainant herself.

- The login to the Crypto.com Wallet App from the new device was confirmed from the Complainant's registered email address by clicking on an email that was automatically generated following the access attempt from the new device, which email contained a link that when accessed, confirms that the owner of the new device has also access to the registered email address of the Wallet holder.

Foris DAX emphasized that as per Terms of Use, the Complainant is solely responsible for maintaining adequate security and control of her login and authentication details. But, considering this, the Service Provider noted that its internal investigation also determined that part of the Complainant's assets related to the unauthorised activity, were trapped into the Crypto.com ecosystem following payment made towards the NFT platform and, as a result, it was able to offer a partial reimbursement of the claimed losses, credited in the form of 0.1997583BTC (Bitcoin) and 772.02 USD Coin (USDC). A screenshot[4] of such reimbursement transaction from the Service Provider's system was also presented as part of the latter's reply. The Service Provider noted that, out of the EUR 15,545.33 lost as a result of the account takeover, EUR8,679.44 were reimbursed.

f) 27 February 2022 – The Complainant disagreed with the Service Provider's decision for the partial reimbursement of her losses. The case was then forwarded to the *Crypto.com* complaints team who acknowledged receipt of the complaint on 2 March 2022.

g) 11 March 2022 – Following an independent review of the Complainant's case, the provider reiterated its stance that the alleged unauthorised access to the Wallet was facilitated by the Complainant herself when she exposed the privacy and security of her personal credentials and, thus, it cannot provide full reimbursement of the reported transactions.

[4] P. 41

Subsequently, the Complainant was provided with the details of the Office of the Arbiter for Financial Services to file an official complaint should she so desire.

The Service Provider submitted that, in summary, it considers that the Account Takeover was a result of negligence from the Complainant which negligence resulted in the exposure of her Wallet's credentials. This is due to the fact that to successfully carry out the reported unauthorised activity, the alleged perpetrator had to be in possession of the Complainant's Wallet passcode and eventually have access to the Complainant's personal email. It further noted that, since transactions done on the blockchain are immediate and immutable, some of the virtual assets in question were lost as they have left the *Crypto.com* ecosystem, and hence the reason of the partial reimbursement of the losses incurred.

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

The Complainant and her crypto account

In the original complaint form submitted, the Complainant made reference to two transfers in the *Crypto.com* application, and the creation of an NFT account in her own name. During the cross-examination, she confirmed that she had created the account with *Crypto.com* and had in fact conducted transactions on such account, but insisted that she did not make the three transactions complained about.

The Arbiter notes that despite mentioning two transactions and an NFT account, no detailed explanation of the occurrence has been provided by the Complainant but notes further that this was provided by the Service Provider and its representative.

[5] Art. 19(3)(d)

The latter confirmed[6] that the Complainant became a customer of Foris DAX MT Ltd. upon signing up to use the *Crypto.com* application on 2 February 2021 and agreed to the Terms and Conditions.

The Complainant has originally complained[7] to the Service Provider that on 3 January 2022, transactions were made to NFT and only €300[8] were left in her account but insisted that she did not carry out such activities. She kept asking about the ETH that were held in her account. She also mentioned the fact that she didn't have an NFT account[9] and even enquired about the way it can be accessed.

During the hearing of the 26 September 2022, the Service Provider's representative clearly noted the Complainant's claim:

'… the Complainant claims that her Crypto.com App Wallet was accessed by a third party who performed an unauthorized exchange of 873.408 of the users Cronos token into 0.131482 Ethereum token. Additionally, the complainant reported two unauthorised Ethereum payments of 2.62ETH and 2.502ETH towards the Crypto.com NFT Platform.'[10]

It was also explained[11] that the NFT (Non-Fungible Token) Platform is accessible through a dedicated website through a separate account which any user must sign up for separately to the *Crypto.com* application. To note, however, that the services of Crypto.com NFT Platform are offered by Foris DAX Global Limited which is based in Ireland.[12]

In a nutshell, the alleged unauthorised transactions on the Complainant's Wallet, based on the time (GMT) of the activity, were as follows:[13]

1. -2.621821 ETH – payment towards the Crypto.com NFT Platform;[14]
2. Exchange of 873.4085507 CRO to 0.131482 ETH;[15]
3. -2.502209 ETH – payment towards the Crypto.com NFT Platform.[16]

[6] P. 174
[7] P. 46
[8] P. 48
[9] P. 50
[10] P. 174
[11] P. 173
[12] *Ibid*.
[13] P. 39
[14] P. 27
[15] P. 29
[16] P. 31

The Service Provider's representative witnessed that the total value of the payments to the NFT platform at the material time amounted to approximately €16,000.[17]

Important to note that, considering this information, it transpires that prior to these alleged unauthorised transactions taking place, apart from the amount of CRO that were exchanged into ETH, the Complainant also held some ETH in her Wallet as the first alleged unauthorised transaction was the payment towards the NFT Platform (i.e., 1. above).

During the in-app chat communication, the Complainant herself asked *'Where are my Etheriums?'*[18]*,* but the Arbiter does not have the exact amounts held to be able to reconcile the amounts transacted with the amounts originally held. This is also due to a discrepancy in the Complainant's declaration whereby during the same chat conversation, she stated *'… I can see that my account has no funds in it …'*,[19] whilst at a later stage, she stated *'Yes, I have only €300.'*[20]

The Service Provider

Foris DAX MT Limited 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.[21]

Foris DAX is licensed by the Malta Financial Services Authority ('MFSA') as a VFA Service Provider as per the MFSA's Financial Services Register.[22] It holds a Class 3 VFAA licence granted 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.[23]

[17] P. 174
[18] P. 47
[19] P. 46
[20] P. 48
[21] https://registry.mbr.mt/ROC/index.jsp#/ROC/companiesReport.do?action=companyDetails&fKey=ab2b4261-837f-4d91-8547-e97ed3935ef2
[22] https://www.mfsa.mt/financial-services-register/
[23] https://www.mfsa.mt/financial-services-register/

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'.*[24]

The Application

The *Crypto.com App* is an application which *'… is only accessible via a mobile device' and* offers the account holder *'… a crypto custodial wallet'*, and *'the purchase and sale of digital assets on own account.'*[25]

Observations & Conclusion

Summary of main aspects

The main complaint revolves around the fact that despite noticing that the transactions in question were made from a device with a different IP address and from a different location, same transactions were still carried out successfully. The Complainant is seeking full compensation from the Service Provider as she believes that this was due to a security problem of the *Crypto.com* application.

The Service Provider submitted that the Complainant's request for full reimbursement will not be entertained as it believes that the alleged unauthorised access to her Wallet was facilitated due to the privacy and security of her personal credentials being exposed, and thus, insists that the Account Takeover was a result of negligence on the Complainant's part.

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.'*[26]

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

[24] https://crypto.com/eea/about
[25] P. 37
[26] Example – As per Article 17(e) of the VFAA which deals with *'Where the competent authority shall refuse to grant a licence'*.

Provider is further required to *'ensure that all of its systems and security access protocols are maintained at all time 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 VFAA are the *Virtual Financial Assets Regulations, 2018 (L.N. 357 of 2018).* The said regulations namely deal with exemptions from requirement 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.

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* (iv) & (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 notes 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, minimize 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 recognized cyber security standards, any guidelines issues 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 recognized 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'*[27] 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:

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

…

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., 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 full reimbursement by the Service Provider of the remaining sum allegedly stolen from her crypto account.

The Complainant alleges that Foris DAX failed to protect her account due to security issues of the application.

The Arbiter considers that there is no adequate and sufficient basis substantiating the Complainant's claim in regard to the Provider's security of her account.

The Complainant stated:

'… I created the account with Crypto.com. I say that I have conducted transactions on my account but I did not make these three transactions in question.'[28]

She insisted that:

[28] P. 130

'… I received confirmations by email at the time I made transactions but I did not receive confirmations by email for the transactions that I did not make.'[29]

On the other hand, the Service Provider insisted that on 3 January 2022, the Risk Team detected suspicious logins and transactions on the Complainant's Wallet and, as a result, it was temporarily suspended. Eventually, Foris DAX contacted the Complainant herself via email, and this *'In regards to your security check that we need to complete with you.'*[30]

Both during the hearing[31] of the 21 June 2022 and in the final submissions[32] presented, the Complainant emphasised that she never received any warning or advice from *Crypto.com*, that is, the security control email which the Service Provider claimed to have sent to her email address. Insisted that she could not do anything to avoid the transactions in question.

Whilst the Complainant's claim could not be verified, as these were not even substantiated in any way, the explanation and proofs submitted by the Service Provider are more tenable. Apart from the detailed explanation of the occurrence by the Service Provider both in its reply and as declared by its representative during the hearing[33] of the 26 September 2022, the Service Provider presented an extract[34] of the email communications sent to the Complainant, which shows that on the day on which the alleged transactions were carried out, a total of four emails were in fact sent to the Complainant herself.

As even noted by the Service Provider, the Arbiter believes that this is a case where even the Complainant's email was compromised to the extent that the use of a new device was confirmed through the link of an email reporting use of new device.

The Complainant argued that on her *crypto.com* account, the two-factor authentication was in place, and since any movement should have reached her mobile number, she enquired[35] how the NFT account was created by the hacker.

To this, the Service Provider stated that:

[29] *Ibid*.
[30] P. 163-164
[31] P. 129
[32] P. 179
[33] P. 173
[34] P. 171
[35] P. 179

'… whilst this is correct, the Respondent further highlights that 2-factor authentication did not apply to transactions occurring on the NFT Platform at the material time.'[36]

However, crucial to also note that, based on the Service Provider's declaration regarding the NFT platform, in particular that its services are offered by Foris DAX Global Limited, which is based in Ireland, the Arbiter notes that it does not have any competence to investigate Foris DAX Global Limited's operation.

It has not been made clear why the Complainant expected the two-factor authentication to be made to her mobile rather than to her registered email address. Furthermore, no explanation again was offered why the Complainant took nearly one month to report the loss to the Service Provider and in the meantime did not reply to the latter's emails with security alerts.

Thus, based on the above, the Arbiter does not have enough evidence to conclude that the Service Provider failed to adhere to any specific obligations to safeguard the Complainant's account. In fact, her Wallet and/or account on the *Crypto.com* application was disabled as soon as the same provider detected the alleged unauthorised transactions, sent an email correspondence to the Complainant herself which then remained unanswered, and this even before the same Complainant became herself cognisant of the occurrence and reported this to the Service Provider.

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 full compensation.

However, since crypto currency 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

[36] P. 186

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 in this sector.

The Arbiter considers that much more needs to be done on this front, apart from in other areas, to better protect consumers. Licensed 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. Consumer education is as important and effective as technological safeguards.

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

Alfred Mifsud
Arbiter for Financial Services