Before the Arbiter for Financial Services

Case ASF 147/2021

SK (The Complainant)

vs

Foris DAX MT Limited (C 88392)

(The Service Provider/Foris DAX)

Sitting of 13 October 2023

The Arbiter,

Having seen **the Complaint** dated 19 November 2021[1] relating to the Service Provider's making transfers of crypto assets from his account with Crypto.com to an unidentified external wallet without such transfers being properly authorised by the Complainant for which he is seeking recovery of his loss amounting to €2257.53.

The Complaint

The Complainant stated:

'***I have account LTXXX … XXX3916 associated with Crypto.com app. I was keeping all the login details in strict confidence. On 25 July 2021 around 18:00 my account was hacked Crypto.com app. It was stolen 843.28 USDT, 639.36 ADA, 0.04288ETH***'.[2]

[1] Page (p.) 1 - 53
[2] P. 2

He stated that the Service Provider has refused his claim attributing the unauthorised transfer to his gross negligence, but Complainant not only denies any negligence but asserts that ***'It was fraud'.***[3]

Reply of Service Provider

In their reply, Foris DAX MT stated that:

'Foris DAX MT Limited (the 'Company') offers the following services: a crypto custodial wallet (the 'Wallet') and the purchase and sale of digital assets on own account. 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.

Mr SK (the 'Complainant'), e-mail address: XXX@XXXXX.XX and, subsequently, XXXXX@XXXX.XXX, became a customer of Foris DAX MT Limited through the Crypto.com App and was approved to use the Wallet on the 19th of November 2020.'

They gave the following timeline of events:

25 July 2021

Their Risk team detected suspicious logins and transactions on Complainant's account. The Complainant account was temporarily disabled (after the suspicions transfers were already affected) and the matter escalated to the Complainant.

31 July 2021

Complainant reported missing assets from his portfolio. After proper re-identification of the Complainant, the report was considered as an alleged account takeover (by unauthorised persons/fraudsters) and further information was sought from Complainant.

04 August 2021

Following proper examination, Risk team concluded that the claim was to be declined as there was clear indication that the Complainant had wilfully or

[3] *Ibid*.

unwilfully, by exerting negligence in regard to safekeeping of his personal credentials, facilitated the alleged unauthorised access to his Wallet.

This decision was taken in the context 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 above-mentioned transactions. Our audit trail shows 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 as provided and set by the Complainant himself.*

The login to the Crypto.com Wallet App from the new device used was confirmed from the Complainant's registered email address.'[4]

The hearings

As the Complainant had problems communicating verbally in English, the hearings had to be held in writing through submissions and cross-examination questions to each side.

A lot of information was submitted that is irrelevant to this case and, in the interest of sticking to the substance of the Complaint, the Arbiter will focus on the arguments which are relevant.

The basic points of difference between the parties can be summarised as follows:

1. The Complainant denies any negligence in making available his access credentials to his Wallet whilst the Service Provider maintains that no irregular access was noted until the payments were affected and, consequently, if the payments were not authorised by Complainant himself, they were done by someone who gained access to his credentials through his gross negligence.

[4] P. 62 - 63

2. The Complainant maintains that the Service Provider was bound by European Payment Services Directive PSD 2[5] obligations to enforce strong customer authentication (SCA). The Service Provider maintains that PSD 2 does not apply to transfers of crypto assets as is the subject matter of this complaint and, consequently, has no application to the present dispute. Furthermore, the Service Provider offered the option for its clients to adopt strong 2FA (2 factor authentication) and the Complainant could have opted for such access restrictions.

3. Complainant maintains that he received no email notification about the change of email access engineered without his authority and no notification by email or SMS/phone when the unauthorised transfers were affected. The Service Provider maintains that at the time of the disputed transactions, no changes had been made to the access password or registered e-mail. The fact that Complainant claims not receiving email notifications indicates that he had lost control of his registered email address as the Service Provider had presented evidence that such e-mail notifications had been properly sent.

4. The Complainant makes reference to Terms & Conditions indicating that Service Provider had an obligation to contact him by phone not just by email in case of suspicious transactions and that he had a ***Debit Card Ruby*** with an IBAN number in LT which was never replaced. The Service Provider maintains they are only licensed to hold and transfer crypto assets and that Complainant must be referring to services offered by other members of the Crypto group as they are not LT based and do not issue debit cards.

5. The Complainant maintains that his access codes were always kept secret and never divulged to third parties and, therefore, suspects that transfers disputed could result from internal fraud by Crypto employees. Service Provider maintains that access codes are not known internally to any employee and could only be accessed by the Complainant, or through negligence on his part to carefully protect such access codes.

[5] EU Directive 2015/2366 that entered into force 12.01.2016

6. In fact, the Service Provider states that:

   '*When asked by Customer Services team on 3 Aug 2021 whether he had experienced "any recent events that could lead to one of the following events? A) Hacked email accounts …", the Complainant informed them that "My mailboxes XXX@XXXXX.XX (and) XXXXX@XXXX.XX were hacked (at the same time)". The email address XXX@XXXXX.XX was the Complainant's registered email address at the material time*'.[6]

   This hack was never disclosed by the Complainant, and this tends to dilute his defence of full certainty that his credentials could not have been compromised.

Having heard the parties

Having seen all the documents

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

The Service Provider

Foris DAX is licensed by the Malta Financial Services Authority ('MFSA') as a VFA Service Provider as per the MFSA's Financial Services Register.[8] 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:

[6] P. 146
[7] Art. 19(3)(d)
[8] https://www.mfsa.mt/financial-services-register/

(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.[9]

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'*. [10]

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...'*.[11]

It offers the account holder *'a crypto custodial wallet'* and *'the purchase and sale of digital assets on own account'*.[12]

Applicable Regulatory Framework

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

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

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

The Arbiter further notes that in the year 2020, the MFSA has also issued a *'harmonised baseline guidance on Technology Arrangements'*[13] applicable to its licence holders (including under the Virtual Financial Assets) titled *'Guidance on*

[9] https://www.mfsa.mt/financial-services-register/
[10] https://crypto.com/eea/about
[11] P. 106
[12] P. 60
[13] Guidance 1.1.2, Title 1, *'Scope and Application' of the 'Guidance on Technology Arrangements, ICT and Security Risk Management, and Outsourcing Arrangements'*.

Technology Arrangements, ICT and Security Risk Management, and Outsourcing Arrangements' ('the Guidance').

Further Considerations

The Arbiter is obliged by Article 19(3)(a) of Chapter 555 of the Laws of Malta to ***'determine and adjudge a complaint by reference to what, in his opinion, is fair, equitable, and reasonable in the particular circumstances and substantive merits of the case'.***

Having considered the particular circumstances of the case, including the submissions made and evidence provided, the Arbiter considers that there is no sufficient and adequate basis on which he can uphold the Complainant's request for the reimbursement by the Service Provider of the sum the Complainant claims was transferred to an external wallet from his crypto account without his authority.

The exchange of fiat currency into crypto and withdrawals from one's crypto account, including withdrawals to an external wallet, is an ordinary part of the typical services provided to millions of users by operators in the crypto field such as the Service Provider.

Furthermore, it has not been demonstrated nor emerged that the alleged fraudster to whom the payment was made from the Wallet of the Complainant, was another Crypto.com App user and, thus, a client of the Service Provider in the first place.

The transfer was rather indicated to have been done to an '*external wallet'* and, hence, the Service Provider had no information about the third party to whom the Complainant was transferring his crypto. The beneficiary's wallet of the disputed transfers was '*whitelisted*' as an address by the Complainant or persons who gained access to his account, giving the all clear signal for the transfer to be executed. There is no basis why the Service Provider should have been expected to stop the payments given their relative low value and their proper authentication.

The Service Provider raised suspicions after the transfers were executed following an access attempt made from an unusual location.

Once a transaction is complete and, accordingly, is not in a pending state, the crypto transaction cannot be cancelled or reversed by the Service Provider as provided for and warned in the Terms and Conditions of Foris DAX.

As indicated by the Service Provider, Clause 7.2(b) of its Terms and Conditions regarding the use of the Crypto.com App Services specifies that:

'*Crypto.com processes all Digital Asset Transfers according to the Instructions received from you and does not guarantee the identity of any recipient. You should verify all transaction information prior to submitting Instructions for a Digital Asset Transfer to Crypto.com as the Digital Asset Transfer may not be cancelled or reversed once processed …'*.[14]

It is also noted that Clause 7.2(d) of the said Terms and Conditions which deals with '*Digital Asset Transfers'* further warns a customer about the following:[15]

'*We have no control over, or liability for, the delivery, quality, safety, legality or any other aspect of any goods or services that you may purchase or sell to or from a third party. We are not responsible for ensuring that a third-party buyer or seller you transact with will complete the transaction or is authorised to do so. If you experience a problem with any goods or services purchased from, or sold to, a third party using Digital Assets transferred from your Digital Asset Wallet, or if you have a dispute with such third party, you should resolve the dispute directly with that third party'.*

On the basis of the facts presented during the case, the Arbiter 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.

It is noted that in his formal complaint, the Complainant only referred in a general manner to the regulations and standards applicable to Foris DAX as if it were a normal licensed payment institution offering payments in fiat currencies.

[14] P. 34
[15] P. 35

However, these are not considered applicable, also, given that the Service Provider is not '*a licensed and regulated financial institution'*. Foris DAX is only regulated and licensed as a VFA Service Provider based in Malta 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.[16]

On the balance of evidence provided, the Arbiter concludes that the Complainant has unfortunately fallen victim of an unauthorised hack which gained access to his secret credentials of access to the Cryptom.com App. There is no evidence to suggest that the Complainant himself was party to such scam. On the contrary, it is clear that facilitation to such unauthorised access was unwilful on the part of the Complainant. Unfortunately, however, it is more than probable that it was his negligence in protecting fraudulent access to his credential codes that led to his loss.

Ultimately, the Arbiter does not consider that in the case in question, there is any clear and satisfactory evidence that has been brought forward, and/or emerged, during the proceedings of the case which could adequately corroborate that the Service Provider failed in any of the applicable obligations, contractually and/or arising from the VFA regulatory regime applicable in respect of its business. Nor that the unauthorised access to the Complainant's Wallet could have been a fraudulent inside job of the Service Provider.

The Arbiter 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 still yet to be implemented for the first time in this field within the EU.[17]

[16] 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).

[17] 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/

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 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.

Decision

The Arbiter sympathises with the Complainant for the ordeal he suffered as a victim of a hack, however, in the circumstances of this case, he cannot accept the Complainant's request for compensation for the reasons amply mentioned. The Arbiter is accordingly rejecting the Complaint.

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

Alfred Mifsud
Arbiter for Financial Services