Before the Arbiter for Financial Services

ASF 104/2021

IN ('the Complainant')

vs

Foris DAX MT Limited

(C88392) ('Foris DAX' or 'the Service Provider')

Sitting of the 28 September 2022

The Arbiter,

Having seen **the Complaint** relating to the alleged unauthorised access of the Complainant's account held with *Crypto.com* and the alleged unauthorised transactions undertaken within the said account which led to the Complainant's crypto currency wallet being emptied and his crypto purportedly stolen.

The Complaint

The Complainant explained that on 05 July 2021 he received a notification on Facebook informing him that the *Crypto.com* app had offered him a crypto currency win.

He then clicked on the link via Facebook and found himself on a site that looked completely identical to the *Crypto.com* website with the URL also looking very similar.

The Complainant noted that he entered his login email address and password but on a moment of doubt, he chose not to validate being afraid to be on a malicious platform.

He further explained that during the same day, 05 July 2021, it was not possible for him to connect to his application on *Crypto.com*. The Complainant contacted the customer service of *Crypto.com* the day after, on 06 July 2021, where irregular activity was recognised on his account.

He noted that the security procedure was activated, and he was again given access to his account, only to discover that his crypto currency wallet was emptied.

The Complainant noted that all of his crypto currencies were transferred to Ethereum and that three gift cards of GBP500, GBP100 and another of GBP100 were spent with his money.

The Complainant submitted that he was obviously not the source of this spending.

He also explained that the *Crypto.com* customer service informed him that he cannot be given any further information despite his GDPR rights.

Remedy requested

The Complainant requested a reimbursement of GBP700.[1]

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 crypto purchases/sales 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').

The Service Provider explained that the Complainant became its customer through the *Crypto.com* App on the 10 February 2021 and made use of the wallet services offered by Foris DAX.

The following timeline was provided by the Service Provider:

[1] P. 5 - GBP500+GBP100+GBP100
[2] P. 19-24

a) 6 July 2021 – The Complainant contacted *Crypto.com* Customer Support reporting that he cannot log into the *Crypto.com* wallet app after opening a suspicious link via Facebook.

It noted that during the communication the Complainant claimed that on 5 July 2021 his wallet was accessed by a third party who exchanged ten of his virtual asset holdings (LTC, ADA, EGLD, BNB, XRP, DOGE, XTZ, Link, Dash, CRO) into Ethereum (ETH). The total amount of 0.449315 ETH was then used to facilitate the purchase of three gift cards via the Crypto Pay service offered via the Crypto.com Wallet app.

It explained that the Crypto Pay service allows users to purchase gift cards from various retail outlets which can be redeemed in accordance with the retail outlets terms and conditions. Screenshots of the three gift cards[3] purchased with their corresponding details were included as part of its reply.

The Service Provider explained that upon authentication of the Complainant's identity, including a current selfie photograph provided by the Complainant to this effect, his Wallet was temporarily disabled, and the reported case was escalated to the company's Risk Team for review.

It further noted that 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) 7 July 2021 – The Complainant provided the completed Account Takeover Questionnaire.

Foris DAX noted that following receipt of the ATO Questionnaire its Risk Team reviewed the answers and issued an opinion that based on the facts laid out in the said questionnaire, a reimbursement was to be declined due to clear indication that the Complainant had wilfully or unwilfully, by exerting negligence in regard to the privacy and security of his personal credentials, facilitated unauthorised access to his Wallet.

[3] App Store & iTunes eGift Card of GBP500, of GBP100 and another of GBP100 – P. 20-22

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.

c) 8 July 2021 – The assessment of the ATO case was completed by the Risk Team and their decision was provided to the Complainant via email. The said communication 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 or pass-code used to access your account, which means that whoever accessed your account knew them both.

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.

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.

[4] P. 23

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 noted that the Complainant's Wallet was reopened after taking the necessary steps to secure it:

- The Complainant's registered email address was changed to a new email address provided by the Complainant on 6 July 2021.

- The Complainant's Crypto.com Wallet app password was reset on 7 July 2021.

- The Complainant was also urged to start using 2FA (2 Factor Authentication) and the anti-phishing code security feature available within the *Crypto.com* app.

Foris DAX further remarked that following its decision and feedback provided, the Complainant then requested to be provided with details on how he can submit a formal complaint on the same day.

d) 9 & 16 July 2021 – The Complainant's case was passed on to the *Crypto.com* Complaints Handling Officer who acknowledged receipt of the complaint on 9 July 2021.

The Service Provider's Complaints Officer prepared a final reply which was sent to the Complainant on 16 July 2021. The reply reiterated the Service Provider's position on the requested reimbursement, based on the responses provided by the Complainant, its internal ATO investigation and the conclusions made by its Risk Team. The Complainant was also provided with details of the Office of the Arbiter for Financial Services to file an official complaint should he so desire.

The Service Provider 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 participation of the Complainant.

To successfully carry out the unauthorised activity, the alleged perpetrator had to be in possession of the Complainant's passcode and have access to the Complainant's personal email, which was the registered email address of the Crypto.com Custodian Wallet, both personal credentials being 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.

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 his crypto account

The Complainant, who is resident in France, became a customer of Foris DAX on 10 February 2021 upon signing up for the *Crypto.com App*, as confirmed by the Service Provider.[6]

On 5 July 2021, his crypto wallet had ten virtual asset holdings which the Service Provider indicated were *'worth approximately €833'*.[7]

As confirmed by both parties, all of the Complainant's crypto holdings were exchanged into Ethereum (ETH) on 5 July 2021 and the total holding of ETH was

[5] Art. 19(3)(d)
[6] P. 19 & 36
[7] P. 19, 30 & 36

then used to acquire three App Store & iTunes eGift Cards for GBP500, GBP100, and GBP100 respectively.[8]

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.[9]

Foris DAX is licensed by the Malta Financial Services Authority ('MFSA') as a VFA Service Provider as per the MFSA's Financial Services Register.[10] 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.[11]

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'*. [12]

The Application

The *Crypto.com App* is an application which can be *'downloaded and installed on a user's enabled device i.e. mobile phone'*.[13]

It offers the account holder *'a crypto custodial wallet'* and *'crypto purchases/ sales on own account'*.[14]

[8] P. 3, 12-13, 19-22
[9] https://registry.mbr.mt/ROC/index.jsp#/ROC/companiesReport.do?action=companyDetails&fKey=ab2b4261-837f-4d91-8547-e97ed3935ef2
[10] https://www.mfsa.mt/financial-services-register/
[11] https://www.mfsa.mt/financial-services-register/
[12] https://crypto.com/eea/about
[13] P. 37
[14] P. 19

As indicated by the Service Provider, *'accounts cannot be accessed through the official Crypto.com website'* [15] and the *'only way to access a Crypto.com account is through the Crypto.com App'*.[16]

Observations & Conclusion

Summary of main aspects

As explained during the Complainant's cross-examination at the hearing of 8 February 2022, the Complainant sought compensation from the Service Provider as he considers that Foris Dax should have secured his account and not allowed unauthorised parties to access his account.[17]

During the same hearing, the Complainant confirmed that his *'complaint is for being a victim of fraud and scam vis-à-vis a separate website that looked similar and extracted [his] login details'*.[18]

As testified during the hearing of 15 March 2022, the Service Provider believed that the Complainant *'has been scammed'* and it was *'not challenging him that he did this'*, [19] despite that in its reply, it noted that the account takeover could have possibly been the result of *'wilful participation of the Complainant'*.[20]

As confirmed during the same hearing, the Complainant's account *'had been accessed with his credentials from a different device and a different IP'*, where the logins with the Complainant's credentials *'appeared to have been done from France'*.[21]

As detailed in its submissions, Foris DAX nevertheless considers that the Complainant should be responsible for the lost crypto on his account given that it claims this occurred as a result of his negligence.[22]

[15] P. 36
[16] P. 37
[17] P. 27
[18] P. 28
[19] P. 31
[20] P. 24
[21] P. 31
[22] P. 22 & 24. The Service Provider even mentioned *'gross negligence'* on the Complainant's part in its final submissions – P. 37.

In essence, the Service Provider submitted that both the personal credentials, these being the Complainant's registered email address and passcode, that were used by the party to access his account and undertake the alleged unauthorised transactions were in the Complainant's *'sole possession'*.[23] It claimed that the Complainant was negligent in maintaining *'the privacy and security of his personal credentials'*, [24] after *'opening a suspicious link via Facebook'*.[25]

The security of access to the Complainant's account was apparently jeopardised when the Complainant clicked on a Facebook notification which informed him that he had a crypto currency win. Following that, he was directed to a site which looked identical to *Crypto.com* and had a similar web address. The Complainant inserted his email address and password on this similar, but counterfeit platform, but noted that he did not *'validate'* this information as he was afraid this was *'a malicious platform'*.[26]

The Complainant took prompt action and contacted the Service Provider within a day, the 6 July 2021, but this was nevertheless too late as his crypto wallet had already been emptied through the conversion of his crypto holdings into another crypto currency which was then used to purchase a number of gift cards.

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'*.[27]

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

[23] P. 24
[24] P. 22
[25] P. 19
[26] P. 3
[27] 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 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.

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'*[28] 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., 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

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

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 his crypto account.

This is when taking into consideration various factors including the following:

(i) ***Nature of Complaint, activities involved and alleged shortfalls***

As outlined during the hearing of 8 February 2022, the Complainant's *'…. complaint is for being a victim of fraud and a scam vis-à-vis a separate website that looked similar and extracted [his] login details'*.[29]

Although it is not clearly spelt out in the Complaint Form, the Complaint, in essence, involves the claim that the Service Provider did not have adequate systems in place to prevent the unauthorised access or takeover of his account by third parties.

Indeed, during the hearing of 8 February 2022, the Complainant claimed that the Service Provider failed him in that his *'account was not secure by the company'* and he re-iterated *'that the company should have secured [his] account'*.[30]

No satisfactory and sufficient details were however provided by the Complainant of the reasons why he deemed his account as not being properly secured by Foris DAX.

It is noted that in his final submissions, the Complainant highlighted *inter alia* that the Service Provider was '*able to recognize that the connection IP address was different from the one usually used'*, and that *'the different actions of conversion towards ETH are abnormal compared to [his] usual activities, where [he did] not carry out so much transaction'*.[31] In the said submissions, he thus questioned whether *'an alert on this [un]usual activity'* could *'have been activated'*.[32]

[29] P. 28
[30] P. 27
[31] P. 32
[32] *Ibid*.

It has not been demonstrated, however, that the Service Provider was subject to such obligation and monitoring in the first place, and even if it was, the Arbiter does not have sufficient comfort either that an alert, on its own, would have stopped the Complainant's crypto assets from being stolen given the particular circumstances.

Moreover, the claim that the unauthorised transactions were abnormal compared to his usual activities was not substantiated.

The use of a different IP address to login into the account is also not reasonably expected to automatically trigger, on its own, a blocking or freezing of an account either. This is even more so when the login *'from the new device was confirmed from the users registered email address',* as submitted by the Service Provider and uncontested by the Complainant.[33]

The Arbiter also notes that, as indicated in the Service Provider's email to the Complainant of the 8 July 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'*.[34] This would have made his account more secure but were, regretfully, not implemented by the Complainant.

The Complainant himself admitted that he was tricked to enter his personal credentials (login email address and his passcode) on the pretext that he had a crypto-currency win. It is obvious that the Complainant was a victim of a scam and since these transactions were made by the fraudster using his credentials, the Service Provider could not trace anything abnormal being taking place.

However, the Arbiter does not agree with the Service Provider's assertions that the Complainant's loss was the result either of his negligence or because of his wilful participation in the scam. One has to consider the scenario at the time of the transaction and the

[33] P. 23
[34] *Ibid*.

psychological state that the Complainant found himself in. It is true that he should not have given his credentials so easily but, unfortunately, human nature is what it is: he believed the scammer's lie and fell victim to it.

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 indeed still yet to be implemented for the first time in this field within the EU.[35]

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.[36]

(ii) ***Lack of satisfactory evidence on key aspects***

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

[35] 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/

[36] 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

more when the unauthorised logins with the Complainant's credentials were '*done from France'*, as confirmed by the Service Provider during the hearing of 15 March 2022.[37]

As outlined above, the Complainant's case is further weakened when no satisfactory evidence has been brought forward by the Complainant, 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 regulatory regime applicable in respect of its business.

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

In the case in question, the Arbiter does not consider that there is clear and sufficient evidence that the Service Provider has not adhered to the applicable requirements detailed under the section *'Applicable Regulatory Framework'* as summarised above.

Neither has it emerged that the local regulatory regime applicable to the Service Provider imposed a mandatory requirement for the application of Strong Customer Authentication[38] to access an account.

In the circumstances, the Arbiter cannot accordingly determine either that the Complainant had a reasonable and legitimate expectation for the Service Provider to mandatorily apply a higher level of security such as two-factor authentication, 2FA, 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 himself - either because he was not aware of such feature or because he consciously opted not to apply it.[39]

[37] P. 31

[38] 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)

[39] Email of 8 July 2021 of the Service Provider – P. 23

The Arbiter further notes that the regulatory framework does not include either any specific provisions 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.[40]

Decision

For the reasons amply explained above, the Arbiter is accordingly rejecting the Complainant's request for 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 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

[40] Example - Articles 73 and 74 of the EU's Payment Services Directive (PSD 2).

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