Before the Arbiter for Financial Services

Case ASF 051/2022

~~Belal Sultan~~EF

~~(Holder of Passport No. 522369330)~~

~~—~~('the Complainant')

vs

Foris DAX MT Limited (C 88392)

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

Sitting of the 26 May 2023

The Arbiter,

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with *Crypto.com*, where his crypto assets holdings were exchanged into other digital asset/s (crypto) and subsequently withdrawn to an external wallet address, resulting into his crypto assets being purportedly stolen.

Background to The Complaint

The Complainant explained that he was an investor on the Service Provider's platform and that an incident occurred in relation to his holdings of crypto assets.

He explained that

"My app was hacked on 28 November 2021. The hacker managed to change to sell cryptocurrency coins the transfer to another account. In normal circumstances when I create a transaction, I receive a mobile text notification as well as an email (The emails can be found on my mobile and on my office

computer). If I were to sell a coin am also asked to confirm either my fingerprint or 2FA (which was active on the day). On this evening, all notifications and emails didn't work not a single email was sent to me. When I complained to the company about this simple fact that their notification system stopped working that night completely, in all their replies they avoided to explain why. It seems to be an internal job as they don't seem to be able to show the notification log for the transactions that took place that evening. They just decided that my account wasn't hacked and that I made the transaction myself."[1]

By way of remedy, the Complainant seeks refund of US$13,880 being the amounts he claimed were transferred to external wallets without his authority.

The Service Provider sent a detailed reply in answer to the Complaint on 31st December 2021 following the Complainant's report of 29th November 2021 about the purportedly unauthorised transactions. In their reply to the Complainant, the Service Provider explained that that upon receiving their Customer report of 29th November 2021, the Complainant's account was immediately disabled, and the complaint was considered as a potentially fraudulent account takeover.

In their reply, the Service Provider explained that as the account was accessed ***"with exactly the same credentials used before the date of the reported incident - the same email address and passcode"*** and that ***"there are no attempts to change the details or failed login attempts. This means that whoever accessed the account has been clearly aware of all of the details.***"[2]

Consequently, the Service Provider declined to offer any compensation or reimbursement for the reported losses.

The Complainant filed his Complaint with the Arbiter on 04 May 2022. The Service Provider filed a reply on 21 May 2022. They explained that Mr Sultan was approved to use the wallet with the Service Provider on 06 Feb 2021 and that on 28 November 2021, the Complainant also opened an account with a sister company registered in Ireland that operates an NFT platform. On the same day, seven rather small holdings of crypto assets and a cash balance of GBP £331 were converted into Bitcoin and together with the existent holding of Bitcoin already

[1] *Folio* 3
[2] *Folio* 8

in the wallet, the total holdings of Bitcoin for a value of about US$ 13880 were used to buy NFT on the wallet of the Irish sister company.

From there these NFT's have presumably vanished without trail as fraudsters are experts in doing, but this could not be confirmed as the Arbiter has no jurisdiction over the Irish company.

In their reply, the Service Provider again refuted any responsibility for the loss sustained and maintained that they consider

"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 Crytom.com Custodial Wallet, both personal credentials that are in the sole possession of the Complainant".[3]

The Hearing Process

The first hearing was held on 22 November 2022, and the Complainant basically related the same issues as included in his official complaint filed with the OAFS. Upon cross examination, when questioned that for somebody to be able to make the disputed transaction on his account, they must have known his password, the Complainant retorted that ***"nobody knows my password. I never give stuff like that. Would you give bank details to anybody? Not even your brother, your family. Why would you give something like that? I was looking into the App ten times a day, and nobody looked over my shoulder to see what I am doing. This is my private investment, and nobody knows about it."***[4]

When asked about inconsistency in claiming that he did not change the password but claiming that he was being bounced out every time he tried to login on that evening of 28 November 2021, and then he managed to see the transactions that were happening, Mr Sultan replied:

"when I started to log in, it kept rejecting my login or go to another screen which was not opening my App but, then, eventually, I logged in and I could see lots

[3] *Folio* 38
[4] *Folio* 79

of transactions and lots of chats; there were about three or four open chats and one of them was asking the officer of Cryto.com some details of my account and why they could not take this money and I could read that.

What I am trying to say is that I did not say I could not log in at all; I was rejected a couple of times until I verified and received a link and managed to log in. The password was not changed and there was a verification process for me to be able to access my account".

At the last sitting held on 10 January 2023, the Service Provider basically restated their defence and explained that purchase of NFT had to be done on the platform of a sister company registered in Ireland. They re-confirmed that all transactions carried out on the Service Provider's platform were all properly authorised, that there was no change of passwords, that access was through the Complainant's registered email link which meant that if it was not Mr Sultan himself, someone had compromised his email account to achieve access to his Crypto.com App.

They further stated that:

Mr Sultan's allegations ***"that he did not receive email confirmations of the transactions occurring from our side"*** were refuted as evidence of such emails were presented in their original response to the OAFS.

"We have shown that the emails were sent successfully after each one of these transactions was performed. So, if Mr Sultan have not seen them, we suspect and we suggest that it was because he had lost completely control of his email account, and someone might have deleted these messages before he saw them".[5]

Consideration

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.

[5] *Folio* 110

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.

The Complainant became its customer through the *Crypto.com* App and was approved to use the Wallet on the 6 February 2021. There is evidence[6] that the Complainant made regular use of the wallet through App access so much so that in the month of November 2021, before the event subject to this complaint, the Complainant made about 80 transactions.

The Terms and Conditions accepted by the Complainant clearly stipulate that he is ***"solely responsible and liable for keeping your Enabled Device safe and maintaining adequate security and control of your login and authentication details …".***[7]

The Arbiter notes that in his complaint to the Office of the Arbiter for Financial Services, the Complainant claimed that the loss of all crypto assets held with *Crypto.com*, which were withdrawn to an external wallet by an alleged unauthorised party, ***"seems to be an internal job as they don't seem to be able to show the notification log for the transactions that took place that evening".***[8]

He further maintained that:

"I have about 5 bank apps that I believe can never be hacked the way crypto.com app was hacked but they don't seem to want to admit that".[9]

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 types of allegations are a matter for the police to handle. Any allegations of criminal fraud should accordingly be reported to the police and relevant authorities.

[6] *Folio* 18
[7] *Folio* 36 and 91
[8] *Folio* 3
[9] *Ibid*.

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 the alleged theft of the crypto assets from his account held with *Crypto.com*;

(ii) The Complainant's claim that Foris DAX failed to protect his *Crypto.com* account and the crypto assets held within the Wallet.

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[10] of the Laws of Malta which stipulates that he should deal with complaints in '*an economical and expeditious manner'.*

The Service Provider

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

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.[11]

Foris DAX is licensed by the Malta Financial Services Authority ('MFSA') as a VFA Service Provider as per the MFSA's Financial Services Register.[12] 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.[13]

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'*. [14]

The Complainant

As already noted earlier, the Complainant had made regular access to his Wallet from the date of his onboarding on 06 February 2021 and also had a blocked account with the Service Provider for GBP 30,000 as security for a Crypto.com Visa card.[15] He can therefore be considered as quite an experienced pair of hands in the crypto ecosystem.

Further Observations

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').

[11] https://registry.mbr.mt/ROC/index.jsp#/ROC/companiesReport.do?action=companyDetails&fKey=ab2b4261-837f-4d91-8547-e97ed3935ef2
[12] https://www.mfsa.mt/financial-services-register/
[13] https://www.mfsa.mt/financial-services-register/
[14] https://crypto.com/eea/about
[15] *Folio* 52

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'*.[16]

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.

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.

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

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"*[17] 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

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

(RTS) on Strong Customer Authentication (SCA) and common and secure open standards of communication."

Conclusions

The Arbiter must choose which contrasting position of the litigants is the more credible, namely:

that of the Complainant that this was more like an inside job and that the Service Provider is fully at fault from his loss because he did not protect his systems against fraud from fraudulent hackers even though he never compromised his credentials for access to his Wallet;

or

that of the Service Provider that the loss was entirely the fault of the Complainant, and what was hacked was not their system but the Complainant's App and email, through the Complainant's negligence and, therefore, the Complainant was fully responsible for the claimed loss as the Service Provider presented documentary proof that whoever accessed the Complainant's Wallet had full access to the Complainant credentials.

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 his crypto wallet account.

The Arbiter considers the replies and documentation provided by the Service Provide to be more plausible than those presented by the Complainant. The Service Provider has submitted satisfactory evidence that the access to the Complainants account were made through accredited credentials and that their system triggered all customary emails which were duly received by the Complainant.

Consequently, there is more credibility to the explanation that the credentials for access to the Complainant's Wallet were compromised from the Complainant's side, rather than that the Services Provider's systems were hacked and failed to

operate with the necessary diligence and precautionary systems as defined by Regulation. This is further supported by the reported unsuccessful attempt by the hackers to obtain release from the Service Provider of the GBP 30,000 blocked to secure his Visa Card.

The Arbiter does take note of the Complainant's assertions that he never compromised his access credentials to his Crypto Wallet. Obviously, the Complainant cannot prove the negative. However, the onus of proof that someone had access to his Wallet even though he never compromised his access credentials lies with the Complainant, once the Service Provider brought satisfactory evidence that all transactions were affected as a result of authenticated access.

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 access credentials.

Sadly, there are various common crypto scams, such as '*Phishing Scams'* and *'Social Media Cryptocurrency Giveaway Scams'* which are used by scammers to obtain the customer's credentials through malicious links and fake websites.[18] It looks likely that the Complainant had unfortunately fallen victim to 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.

(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.[19]

[18] https://www.techtarget.com/whatis/feature/Common-cryptocurrency-scams

[19] Such as the various emails exchanged in December 2021 leading to the final reply from the Service Provider to the Complainant of 31.12.2021 *folio* 8 - 26

(ii) *Allegation that Foris DAX failed to protect Complainant's account and crypto assets*

Taking into consideration the nature of the complaint, the 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 his account and portfolio of crypto assets.

The argument of the Complainant - that he has never been hacked in the several Banking Apps he makes use of - does not prove that the Crypto App was hacked because of the Service Provider's negligence or inadequate security measures.

Furthermore, it needs to be pointed out that Foris DAX is not a regulated bank or 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 banks and financial institutions falling under EU regulatory regimes.[20]

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.[21]

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

[20] 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).

[21] 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/

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.[22]

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

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.

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[23] 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 his *Crypto.com* account, which would have reduced the risk of an account takeover.

[22] 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

[23] 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)

Moreover, as indicated above, 2FA was available to the Complainant at the time of the disputed transactions and was actually availed of by the Complainant which further adds to the suspicion that his credentials were compromised.

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.[24]

Decision

The Arbiter sympathises with the Complainant for the ordeal he suffered due to the loss of his assets, but he cannot accept his 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.

[24] 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.

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. Service providers operating in this field need to also do their part and actively work to improve their on-boarding process by evaluating the much-needed knowledge of benefits and risks 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.

Alfred Mifsud
Arbiter for Financial Services