Before the Arbiter for Financial Services

Case ASF 042/2024

DO

('the Complainant')

vs

Foris DAX MT Limited

Reg. No. C 88392

('Foris DAX', 'the Service Provider' or 'Crypto.com')

Sitting of 25 April 2025

The Arbiter,

Having considered in its entirety, the **Complaint** filed on 12 March 2024, including the attachments filed by the Complainant about his wallet account held with Foris DAX and the transactions involving his wallet.[1]

The Complaint

Where, in summary, the Complainant claims that he is a UK citizen and customer of *Crypto.com*, who fell victim to a sophisticated investment scam in which he was defrauded 26.5 Bitcoin (BTC) which at the time was worth £609,096.14. He explains that he was coerced into using a fake trading platform (of RoyalFX), which mimicked that of a real exchange.

He continues to explain that the scammers took advantage of his vulnerability as he was under stress of selling a house of his father-in-law's estate, coupled with

[1] Complaint Form from page (p.) 1 - 6, and attachments p. 7 - 176

the bereavement due to the passing of the same father-in-law and the constant pressure put on him by the scammers.

The Complainant alleges that *Crypto.com* failed in their duty of care to protect their customers from falling victim to well-known scams, which result in avoidable, wide-scale consumer harm.

He states that he had limited knowledge of Crypto wallets and chose to use *Crypto.com* as it was advertised on the web as under the conduct of the UK FCA, which he understood it to be regulated by the UK.

He alleges a failure on the part of the Service Provider to warn him that his account activity was displaying features that mimicked that of a known scam. He states that *Crypto.com* failed to spot the *modus operandi* of this scam and to intervene in order to protect him, resulting in significant financial loss. The Complainant further claimed that *Crypto.com* failed to adopt the minimum standards expected of a reputable financial firm, thereby resulting in the loss of the Complainant's life savings.

The Complainant noted that after losing all his funds, *Crypto.com* made him aware that the wallet he had been interacting with was likely to be involved in a scam. He additionally claimed that the Service Provider made no further efforts to recover his funds despite the beneficiary wallet being also hosted on the *Crypto.com* platform.

Remedy requested

Consequently, by way of remedy, the Complainant asks for *Crypto.com* to be found liable for the losses suffered and to refund him the sum of £609,096.14 so that his finances are restored to what they were before the scam started.[2]

Having considered, in its entirety, the Service Provider's reply including attachments,[3]

Where the Service Provider provided a full summary of events with the following background:

[2] P. 3

[3] P. 182 – 217 with attachments on p. 218 - 265

"
- *Foris DAX MT Limited (the "**Company**") offers the following services: a crypto custodial wallet (the "**Wallet**") and the purchase and sale of digital assets through the Wallet. 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.*

- *At the material time, Foris DAX MT Limited additionally offered a single-purpose wallet (the "**Fiat Wallet**"), which allowed customers to top up and withdraw fiat currencies from and to their personal bank account(s) for the purposes of investing in crypto assets.*

- *[The **Complainant**], e-mail address xxxx@btinternet.com, became a customer of Foris DAX MT Limited through the Crypto.com App and was approved to use the Wallet on the 24th of January, 2022.*

- *The Company notes that in the submitted complaints file, [the Complainant's] representative has outlined the desired remedy as: (i) reimbursement for incurred financial losses."*[4]

The Service Provider gave a detailed timeline (complete with screenshots from its system) of the transactions undertaken by the Complainant between 25 January 2022 and 22 June 2022.

In essence, it explained that during the said period, the Complainant made a series of deposits in GBP via bank transfers to his Fiat Wallet within the *Crypto.com* App of Foris Dax. On two occasions, a cryptocurrency deposit in Bitcoin (BTC) was also made from an external wallet to his *Crypto.com* Wallet. The Complainant subsequently exchanged the deposited fiat money (GBP) from his Fiat Wallet to Bitcoin. On one occasion, the Complainant also purchased BTC through the *Crypto.com* APP using his personal debit/credit card.[5] The acquired Bitcoin were all then next transferred by the Complainant from his wallet to what *Crypto.com* maintain to be an external unhosted wallet bearing the following address:

3LcSRB8N9XGKeMiXNLfLJfqiRzGUSBGZc8

[4] P. 182
[5] P. 193

Foris DAX explained that between January 2022 to June 2022, a total of BTC 23.9032769 (approx. EUR 1,487,564 based on market conditions as of March 18, 2024),[6] were withdrawn from the Complainant's *Crypto.com* Wallet and transferred to the mentioned external wallet.

The Service Provider further contended that:

> *"Based on our investigation, the Company has concluded that we are unable to honor the Complainant's refund request based on the fact that the reported transfers were made by (Complainant) himself, and the Company was merely adhering to the Complainant's instructions and providing the technical service of transferring the requested assets to the address provided by him.*
>
> *While we sympathize with the Complainant and recognize that he may have been misled or induced into transferring funds to an alleged fraudster, it is important to note that these transfers were made solely at the Complainant's request. We must also emphasize that the address the funds were transferred to does not belong to the Company and as such, any due diligence of the ownership of this address falls under the responsibilities of the provider of said wallet.*
>
> *Unfortunately, Crypto.com cannot revoke any virtual asset withdrawals because blockchain transactions are fast and immutable.*
>
> *While this is an unpleasant scenario, the Company cannot be held liable for the Complainant's conduct, which resulted in him moving his virtual asset holdings to a third party. (Complainant) is solely responsible for the security and authenticity of all instructions submitted through his Wallet as outlined in the Foris DAX MT Limited Terms of Use.*
>
> *Please see the relevant section of the Terms of Use accepted by the Complainant for your reference:*
>
> *QUOTE*
>
> *7.2. Digital Asset Transfers*

[6] In his Complaint, Complainant mentions BTC 26.5 units. See p. 302

...

(b) 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 by Crypto.com unless Crypto.com decides at its sole discretion that the transaction should be cancelled or reversed and is technically capable of such cancellation or reversal. You acknowledge that you are responsible for ensuring the accuracy of any Instructions submitted to Crypto.com and that any errors may result in the irreversible loss of your Digital Asset.

...

UNQUOTE

In summary, it seems conceivable that the Complainant has been the victim of an alleged scam. Whilst we fully empathize with The Complainant in this regard, it cannot be overlooked that he had willingly, according to his statements, transferred his virtual asset holdings from his Crypto.com Wallet to external wallet addresses which he has no access to.

As outlined above in the Foris DAX MT Limited Terms of Use, the Complainant is solely responsible for the security and authenticity of all instructions submitted through the Crypto.com app, and as such, the Company cannot accept liability for the veracity of any third-party or for the instructions received from the Complainant themselves."[7]

Preliminary

As part of the documents attached to his Complaint Form to the *Office of the Arbiter for Financial Services* ('OAFS'), the Complainant provided a copy of a detailed formal complaint dated 24 August 2022, that his legal representatives made with Foris Dax UK Ltd.[8] This was marked by the Complainant as the *'Complaint sent to the Provider'* in the list of Attachments to the Complaint

[7] P. 216 - 217
[8] P. 7 - 19

Form.[9] The copy of the formal complaint provided is addressed to Foris DAX UK Ltd (and includes references in certain instances to the regulations of the FCA in the UK). As part of the attachments, the Complainant included a copy of (an undated) letter sent by the Group General Counsel of *Crypto.com*.[10] He marked this letter in his Complaint Form as being the *'Crypto.com rejection letter'* and the *'Final Letter from Provider'*.[11]

It is noted that the said letter from the Group General Counsel of *Crypto.com* explains *inter alia* that the Complainant's *"Crypto.com App account was serviced by Foris DAX MT Ltd"*.[12] It further stated that *"the governing law and jurisdiction is Maltese Law and the proper dispute resolution procedure is by arbitration".*[13] The Group General Counsel also confirmed that they *"would not object to OAFS arbitration on this occasion"*.[14] A complaint was eventually filed by the Complainant with the OAFS.

The Arbiter considers that, for the purposes of Cap. 555, the substance of the complaint is, in the circumstances, considered to have been communicated to the Service Provider, Foris DAX MT Ltd, and the latter had a reasonable opportunity to deal with the complaint in question. This is also when taking into consideration the following:

(i) The nature of the Complaint as explained by the Complainant in the Complaint Form which, in essence, reflects key issues raised in the formal letter of complaint provided;

(ii) The reply sent by the Group General Counsel of *Crypto.com* and the direction it itself gave to the Complainant that *Crypto.com* would not object to OAFS arbitration;

(iii) That the Service Provider made no claim in its reply to OAFS received on 21 March 2024,[15] that the customer had either failed to communicate the substance of the complaint to it or that it was not given a reasonable

[9] P. 6
[10] P. 20
[11] P. 6
[12] P. 20
[13] *Ibid.*
[14] *Ibid.*
[15] P. 182

opportunity to deal with the complaint prior to the Complaint filed with the Arbiter.

Any references made in the formal complaint sent by the Complainant to *Crypto.com* to requirements applicable under the FCA's framework shall not be considered insofar as they are not relevant and not similarly reflected in the local rules and requirements applicable to the Service Provider.

The Arbiter shall next proceed to consider the merits of the case.

The Merits of the Case

The Arbiter will decide the Complaint by reference to what, in his opinion, is fair, equitable and reasonable in the particular circumstances and substantive merits of the case.[16]

The Arbiter is considering all pleas raised by Foris DAX 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[17] which stipulates that he should deal with complaints in '*an economical and expeditious manner'.*

Considerations

The Complainant

The Complainant described himself as a *'semi-retired, working on a part-time basis as XXXXXXXXX'* who is *'74 years of age'*.[18] It was indicated that he was XXXXXXXXXX, where he *'was bombarded throughout by RoyalFX essentially demanding he deposits more money'*.[19]

Background about the scam

The scam occurred over six months from January to June 2022. The scammer first skilfully gained the Complainant's trust and friendship, as evidenced by the multiple messages exchanged between the Complainant and a *'crypto manager'*

[16] Cap. 555, Art. 19(3)(b)
[17] Art. 19(3)(d)
[18] P. 26
[19] P. 8

– a purported representative of RoyalFX.[20] Various messages and calls occurred between the Complainant and the scammer, where the communications revolved not just about trading but also on other aspects, including claimed common interests.

Forex positions (such as in Yuan, USD vs Rub), digital currency (such as E-krona) and crypto (bitcoin) trading were *inter alia* discussed during such communications, with the scammer frequently also sending market updates and news about crypto and the economy to the Complainant to deceivingly portray professionalism and encourage him to invest more money.

The Complainant even introduced his wife and friends to invest with the scammer.[21] He started with relatively small amounts for investment and initially had no intention to increase the amounts invested.[22] However, the Complainant was along the way, skilfully persuaded to channel more and higher amounts of funds with the excuse not to lose the purported investments and gains he was led to believe that he had made.

To lure him into continuing to make payments, the scammer convinced him that he must first settle margin, insurance, tax, upfront fees and liquidity requirements for the release of his purported profits.[23] The Complainant ended up selling part of his assets and taking out loans (on his assets, and seemingly from family members/friends) to get funding to settle the requested payments.[24]

The Complainant explained that he also gave access to the scammer to his computer through the AnyDesk application. In his witness statement, signed and dated 25 September 2023, the Complainant stated that:

> *"I was not in control of what happened to the funds following my deposit to the Intended Defendant's platform, as the scammer who was conducting the authorised push payment fraud used Anydesk on all the transactions to help me use my Crypto.com wallet. He also had the 2nd part of the 2FA and*

[20] P. 125 - 176
[21] P. 129 & 134, 135, 136
[22] P. 132
[23] E.g. - P. 146, 152, 158, 170
[24] P. 154, 171/172, 308, 314, 315, 375, 386

> *showed me another platform where it appeared my investments were going up."*[25]

The case in question is typical of what is commonly referred to as a pig-butchering scam. In the circumstances, the Arbiter has no reason to doubt, even on the balance of probabilities, the veracity of the Complainant's claims that he was a victim of a sophisticated scam. No reasonable doubts emerged in this regard, nor were they raised by the Service Provider, that this was not the case. This is also when taking into consideration the particular circumstances and various factors as emerging during the case, including: the nature and credibility of the events as outlined in the complaint; the witness statement;[26] the testimony during the hearings of the case and the evidence emerging during the proceedings; the nature and extracts of communications with the scammers;[27] official statements provided and correspondence exchanged with *Crypto.com*, including the Complainant's emails of 19 April 2022,[28] 12 May 2022,[29] 17 June 2022[30] amongst others.

All the various factors reasonably support the claim of fraud, and that the Complainant fell victim to a sophisticated scam.

Hearings

During the first hearing on 7 October 2024, the Complainant *inter alia* submitted:[31]

> *"… I just point out that when I discovered that I was being scammed, it was right at the very end of quite a lot of money.*
>
> *And it was only when the Cybercrime Police from my local county actually came to the house and told me it was a scam, that I realized it was a scam. So, up to that point, I was convinced it was a genuine operation …*

[25] P. 28
[26] P. 26
[27] P. 125 - 176
[28] P. 363
[29] P. 386
[30] P. 390
[31] P. 266

When I started talking to the Royal FX, they said that they did all their monies come in and out via a Wallet. They go through the Bitcoin process. So, they said to me, 'You'll need a Wallet.' So, I went on to the websites, googled Crypto Wallets, and Crypto.com came up. I think it was almost at the top. It stated that they were regulated by the UK's Financial Conduct Authority. It seemed good to me, so I applied for a Wallet.

When I told the Royal FX that I got a Crypto.com Wallet, the reaction from Oscar White was, 'I wouldn't have got one of those. But, however, if that's what you've got, that's what we'll use,' and that's how I came across Crypto.com.

It's fair to say that at the time, I was just an absolutely, totally, inexperienced investor, had no real clue about cryptocurrency and what I was interacting with.

I wanted to invest in E-Krona. I felt it was just a dabble, if you like, a long-term investment. It's backed by the Swedish bank. So, I just googled 'Investing in E Krona'. It came up. Somehow, through the process, the Royal FX contacted me, and I can't recall exactly how that process worked.

I must have gone to a provider and then, somehow, they came back, contacted me. And said, 'You know, we deal in E-Krona'. Fine, that sounds good. In fact, they said we're one of the few trading houses that can deal in E-Krona. So, I thought that seemed fine and, so, I started to use the Royal FX and they set me up with an account.

They set me up with the ability to look at trades and, initially, they wanted me to trade myself. They said, 'You will get some calls. We'll instruct you as how to trade and use our platform and you can trade yourself.'

And I said, 'I'm not a trader. I know nothing about it. I just want to invest some money in the E-Krona. So, you know you're the traders. You're the experts. You do the trading,' and that's when they put me onto Oscar White. And we started from there.

When I first started using Crypto.com, I was given a declaration to say what I was planning on using the services for. I've got it in front of me actually. Crypto, through their website, asked the questionnaire. It asked, 'How did I

learn about crypto?' I put, 'From my trader.' It wasn't Crypto.com Wallet from my trader, it was, 'You need a crypto Wallet.' I did it on my own, not coerced.

I put down, 'I'm only trading with the Royal FX and it was to make a profit with the Royal FX'. And, 'Am I planning on trading or investing in Forex trading?' And 'What company am I working for?' The Royal FX wrote. 'How much per month would I be buying?' I put '£100 a month'. I wasn't planning on investing huge sums of money and it says, 'Have you communicated with crypto?' And I said, 'E-mail and WhatsApp'. That was it and signed.

I don't have a date on it. It was in and out of their portal, but I think it was about December 2021. But without their portal being available to us to see exactly, I can't be precise on that.

I assume this document is to determine the KYC information about customers that are planning on using Crypto.com at the time. Obviously, I have given several points of notice here on the platform I am engaging with, which was Royal FX. And I have also said the amount I would be using monthly is only going to be £100 which was obviously massively exceeded during this time. I believe during April I also got several questions about the source of my funds.

Crypto.com asked me on more than one occasion - and, again, I don't have the dates because it's within their portal and they haven't advanced the portal for us – in fact, they asked on several occasions where the money was coming from. They wanted bank statements. I believe they wanted three months' bank statements which I supplied. I supplied where the money was coming from. They asked me later on, as more money was going through, where that money was coming from, which I supplied; and for every question they asked me, I had an answer for.

I say that I have got throughout the correspondence from April till August and I've got about eight points of notice where I informed them about Royal FX and I asked some questions about who I was engaging with at any point.

Asked by my representative whether they gave me any information on who Royal FX were or made me believe I was involved in a fraud, I say that they

gave me information. I think it was August time where they said to me, 'We think that the Wallet that you're putting money into is a scam'. In fact, I think I asked them previous to that, 'Do you know anything about the Royal FX? You know, have people got money out of them?' And they said, 'We can't divulge other clients' transactions,', which I suppose is fair. But I asked them specifically, 'What makes you think this is a scam?' And at that time the Wallet was frozen and then, a couple of emails later, they said, 'Your Wallet's unfrozen, carry on!' and they never did.

They've never told me why they thought it was a scam to this day.

I say that from December 2021, when I signed the declaration and I initially let them on notice about the Royal FX through to August, when pretty much all of my money had been drained, I never provided any information about the platform I was dealing with. Crypto never said anything at all. Only, if they ever intervene, they just asked where my money was coming from. I always said where it's coming from and where it was going to, and it was all going to the same place all the time.

Asked by my representative if they ever froze my account during verifying the source of my funds and I had to send them back the statements and whether my activity was suspended or was I allowed to continue sending out money, I say that on a couple of occasions, they implied that my account was frozen, but I was not transacting at the time, so it wasn't actually impacting me. Then they say, 'Your Wallet is open again and you can use it.' It was a very, very short time span, exceptionally short. It made no difference to me because I wasn't actually having to do anything at the time as it happened.

So, they conducted checks on the source and destination of my funds and allowed me to continue sending money to the platform.

Another thing we have an issue with is just that we believe that the Wallet is hosted on Crypto.com's platform. We asked Crypto.com to verify if it was one of their Wallet addresses to which they replied, 'Yes, the Wallet address provided is a valid deposit address for Crypto.com.'

I was convinced I was sending it to the Royal FX platform. They said, 'If you want to deal with us, you need a Wallet.' I wanted to deal with them, so, I got a Wallet; you know, it's a bit like somebody saying, 'If you want to deal with us, you must have a bank account.' So, you go and get a bank account. I had no idea of the intricacies that goes on with Crypto. I wasn't really interested in Crypto per se. I was just interested in investing some money with E-Krona.

I say that the scammers were really, really clever. I mean our cyber police said it's one of the most sophisticated scams they've ever come across. They put me under immense pressure to come up with funds to release funds like liquidity when the cyber police came in and said, 'Listen, if you put more in, you're going to lose it up. You're losing it anyway'.

So, that's when I realised it was a scam and from that point on, life just sort of crashed; you can imagine, I lost 9 kilos in weight. I couldn't eat, couldn't sleep. I was in the process of doing a guitar exam, a Grade 6 exam that went out the window. I couldn't concentrate and still can't concentrate on that now today. Highly embarrassed, absolutely devastated.

Luckily, my wife understood, you know, as she said, 'You've done nothing wrong.' What have I done wrong? I hadn't done anything wrong. And yet, I'm in a situation where I have thrown away all that money. Everybody seemed to say 'Yeah, it's alright. It's all legit. It's all gonna work.' I believed it was legitimate right to the very end. I had no cause not to. I even told the Royal FX, 'Listen, you've got some bad reviews.' And he said, 'Yeah, you showed me a large company that hasn't got a bad review.' If you look at Crypto.com reviews on Trustpilot now, it's worse than Royal FX was, you know; their reviews are appalling. And yet, you know, it was so professional and then you suddenly discover that it was all a scam.

It's taken 18 months to get my life back. I did get my weight back. It took about a year and a half. And we're coming to terms with what we've got now. We've still got a horrible debt to pay. I still owe a creditor. I still have a mortgage. And whereas life should have been going really, really well, it's not. I'm still working now; I'm in Budapest now working. So, yes, it's been horrible, absolutely horrible. Time is time. Time is a healer, but I still think

about it every day. That's the problem. It's never out of your mind. It's always creeping into your mind. It's ghastly.

The police did a trace, I think, regarding how much money had been lost by the Royal FX scam. I did speak to them very recently actually, and I think around about £1.6 million went through that Wallet. And then, it went out of that Wallet and was dispersed around, basically, laundered and fled out to about 20 or 30 different Wallets. And it was mixed up with other people's Wallets. But they did say that it was very, very sophisticated, very clever, very clever.

The Arbiter asks me when transferring my money to Crypto.com Wallet whether they were bank transfers. I say, yes, and they were from my bank in the UK.

And, yes, I would always transfer them from the same bank.

Asked by the Arbiter if I made a claim against the bank for not warning me that something was wrong when I was sending so much money to a Crypto Wallet, I say I would like CEL[32] to answer this question."[33]

The Complainant's representative stated:

"*A complaint was made to the bank which was rejected on the grounds that it was a Me-to-Me Payment. Obviously, the last financial institution that saw these funds before it went to a scam platform was Crypto.com. The onus should be on them as a platform that handled it before it went to the scam platform, not the bank, who simply listed a payment from.*

The bank in the UK was HSBC. So, we did make a claim against that. We went through the Financial Ombudsman Service in the UK but, ultimately, it was rejected and upheld for that reason that it was a Me-to-Me Payment and the Crypto.com account because [the Complainant] set it up himself and operated that at the time, it's essentially a transfer to him, and then HSBC didn't accept responsibility for what happened after that stage.

[32] CEL being lawyers representing him: Cheshire Estate & Legal Limited trading as CEL Solicitors.
[33] P. 266 - 271

Yes, there is an FSO decision on this case and we can send this through to the Arbiter."

The Arbiter requested to see the FSO decision[34] and asked further questions to the Complainant, to which the Complainant answered:

"*… I mentioned that my intention was to invest in E-Krona.*

The Arbiter asks whether a normal retail investor knows what E-Krona is. He says that it gives him the impression that I had some good background of investments if I wanted to invest in E-Krona.

I say, no, I had no background on investments on E-Krona. I've been looking at E-Krona. E-currencies was something that was starting up, I believe, around a bit before that time. And I've been looking at E-Krona, and there's also been a fair amount of news about Bitcoin and how that was going. I felt because E-Krona was backed by a bank, it actually had a backing. It actually had some, you know, there was some solidity behind it. It's a bit like our currencies, really. And I just thought, I had a little bit of spare cash. I thought, interest rates were dreadful. In fact, you were almost getting nothing for your money in the bank and I thought, well, I'll pop some money in there. It seems to be a reasonable investment. We're not looking for huge percentages. We're only looking 5%/6%/7%/8% would be nice. And that seemed to me, reading on what I read about E-Krona and the way E-currencies were going, that might well be a good investment; but as far as investments are concerned per se, I know nothing of investments. I leave that to my financial guys."[35]

Under cross-examination, the Complainant further submitted *inter alia* that:

"*It is being said that before I chose to open my Wallet with Crypto.com, I had done my due diligence, I had researched and read about it, and I found that this would be the platform that I wanted to work with.*

Asked whether I also googled Royal FX before I decided to trade with them, I say, yes.

[34] P. 271
[35] P. 271 - 272

Asked what I found, I say I found much the same as your Trustpilot. There were some really good ones, and there were some really bad ones.

And I did actually quiz the Royal FX in the early stages and said, 'You know, you've got some bad reviews'. And the guy said, 'Yes, you show me a company, a large company that's international, does a lot of business, that hasn't got a bad review!' and that's absolutely true. There's always somebody that's unhappy. There always will be some bad reviews.

The one thing that swayed me for Crypto was it's regulated by the FCA. As far as the Royal FX is concerned, they came up and said, 'Yes, you could do E-Krona.' They spoke to me, they sounded exceptionally professional and, therefore, I had no reason not to go with them. You know, if you start googling things you can be swamped. I wasn't interested in being swamped. These two seemed good to me. That's where I was going.

Asked whether apart from some bad reviews on Trustpilot, I saw any other warning signs such as the FCA warning me that this was a fraudulent company, something of that sort, I say, no, I didn't see. I didn't go further than that. I didn't have any reason to go further than that.

It is being said that I mentioned that I had actually believed that Royal FX was a legitimate trading platform up until the police came to my home to inform me that I had been a victim of a scam.

Asked whether I remember what date that was, I say that the date the police came in, I think was in August. I think it was either the end of July or August. What happened was that the bank sent round the policeman to check that we were OK. We explained what we were doing to the policeman. And he said, 'I'll report this to Cybercrime'.

And a couple of days later, came a Sergeant and his assistant from Cybercrime, and they said to me, 'This is definitely a scam.' I had another little bit of money to pay that I believed was going to release the funds, and they said to me, 'If you put it in, you'll lose it.' So, I didn't put it in, and that's when I then questioned the Royal FX and said, 'Listen, you guys scammers, I've actually got the cyber police here!' and bam! everything shut down.

I say this was in August 2022.

I confirm that after I decided to open an account with Crypto.com, I deposited funds from my bank account into my Crypto.com Wallet which I then traded for Bitcoin, and then I sent it off to what I believed was Royal FX.

Asked who gave me the instructions to do so, I say Royal FX did. Royal FX said that this is how we get the money into our accounts. …

… Asked who provided me with the Wallet address to transfer the Bitcoin from my Crypto.com account, I say, Royal FX did.

Asked whether in my opinion, Crypto.com carried out my instructions as instructed by me through the Crypto.com app, I say, yes, it did.

It is being said that I mentioned that I have finance guys and that I leave it up to them to decide investment matters.

Asked whether I asked them before for advice on the Royal FX, I say, no. The finance people I have are literally my pension provider and they just deal with my pension. So, I had no reason to go there. I wasn't using any pension money. I didn't ask them. In hindsight, that would have been a clever idea.

I am being referred to what I said that a police department had investigated the scam …

… basically, in conclusion, they said that the Wallet address provided to me by Royal FX was fraudulent.

I say, well, it wasn't. I can't say that it was fraudulent. Must have been a genuine address because money went into it, but it was being used fraudulently."[36]

Further to additional clarifications requested by the Arbiter during the said hearing:[37]

a) The Complainant confirmed that as a remedy he was seeking a refund of all his losses to the amount of £609,096.14;

[36] P. 272 - 274
[37] P. 274

b) The Complainant explained that he was not able to give the Arbiter with a date when the Service Provider froze his account for a short period of time as he did not have access anymore to any of his conversations over the Crypto.com platform.

c) The Complainant's representative stated that they were under the impression that the Wallet managed by the fraudsters was a Wallet hosted on the *Crypto.com* platform given that when they asked one of the representatives where it was a valid deposit address, they responded positively, and that the wallet address provided was a valid deposit address for Crypto.com.

   However, the Service Provider's representative clarified during the hearing that the "*Wallet was an external Wallet address not hosted by Crypto.com*."[38]

During the hearing of 7 October 2024, the Arbiter also requested the Complainant to provide a reference to the case decision from the FSO. This was again asked for in the Arbiter's decree of 7 November 2024.[39] A copy of the FSO's decision, including the Complainant's comments on such decision, was presented on 11 November 2024.[40]

Following the presentation of certain documentation outside the case hearings, the Arbiter considered the parties' further submissions during the hearing of 13 November 2024.[41] Following the said hearing, the Arbiter issued a decree dated 15 November 2024, wherein it was *inter alia* decided what new evidence was to be allowed in the process and what documents were to be disallowed and expunged from the proceedings.[42]

In the decree of 15 November 2024, the Arbiter also requested the Service Provider to present:[43]

[38] P. 276
[39] P. 288
[40] P. 289 - 292
[41] P. 293 - 300
[42] P. 301
[43] P. 302

> *"1. Copies of documents submitted by the Complainant during the onboarding process for KYC purposes and any documents submitted by the Complainant during the course of operations of the relationship.*[44]
>
> *2. Copies of in-app chats with the Complainant during KYC and during the course of operations of the relationship*."[45]

In the said decree, the Arbiter sought additional clarifications regarding the amounts claimed to have been transferred out from *Crypto.com* and, also, requested the dates when the account of the Complainant was temporarily frozen for reasons of (enhanced) due diligence on the account holder.[46]

Hearing of 4 February 2025

During the final hearing on 4 February 2025, under cross-examination, the Complainant *inter alia* submitted:

> *"It is being said that … in March of 2022, I had called the bank and informed them that I wanted to report a scam. On 9 March of the same year, 2022, I phoned them back and said that I was convinced that this is not a scam.*
>
> *… from March to April, there were a number of transactions and in or around April 2022, the bank informed me that it was sceptical about this transaction and it was sceptical about the investment that I had been saying that I was going to do it for Royal FX and that I said, according to the decision, that I would take responsibility for my actions.*
>
> *It is being said that from April to June, most of the transactions took place and there was a material number of transactions that I decided to go ahead with. So, in my cross examinations, I said that I found out that I was scammed very late in the day. And it is being quoted, 'When I discovered that I was scammed, it was right at the very end of quite a lot of money.'*
>
> *It is being said that in actual fact, I first had an indication of a scam, that I might have been scammed, way back in March when I made my first phone call to HSBC and then, again, in or around April, where a paid for financial*

[44] Submitted p. 305 - 323
[45] P. 324 – 414 with clarification p. 415 - 416
[46] P. 302 & 417

advisor and the bank told me that they were not convinced that these transactions were safe.

So, I am being asked whether it is not really correct to say that it had not been very late in the day, as I say in August, but much earlier that I had an indication that Royal FX could have been a scam.

In answer to that, I say that I went to a pension provider to ask for some money to put into this investment company. They have no experience in crypto whatsoever, which they admitted they had no idea of crypto. They would not, as a pension provider, allow me to do anything with crypto, period. That was the end of the story. Whether it'd been legitimate, illegitimate or whatever, they would not take any money out of the pension or any crypto transaction. They suggested it might be a scam. So, they suggested I should report it, which I duly did.

So going on from that, the Royal FX said, of course, nobody wants to deal with crypto at the moment because the normal banking is losing millions to crypto investment which seemed reasonable to me. I double checked it all, looked at it all and I thought I can understand if people don't understand crypto, I don't understand crypto. It still seemed very legitimate to me. Everything seemed absolutely reasonable: the timelines, the investments, the way they were going. There was nothing to suggest that this wasn't going as it would normally go.

So, I called the bank again and said, 'Look, I'm not convinced,' and I would make a comment here: the bank never, never once said to me, 'We think this is suspicious.' Not once. I've had nothing from the bank at all. They just asked me, 'You sure you want to invest in this?' 'Yes, I'd like to invest in this.' They didn't say, 'Do you think you should check it out? We think it's suspicious.' If they had thought it was suspicious, they probably would have stopped the payment going.

It is being said that from the decision, it transpires that in early March I already had a feeling, that I knew someone told me that this was a scam and yet, I was convinced the next day and phoned back and said I was not convinced anymore and that I wanted to proceed.

Also, that around April, again, the bank or whoever was advising me on the other side, it transpires from evidence produced in front of the Ombudsman, (which the service provider does not have but in the judgement, it seems clear) that they informed me that they were sceptical and that this did not make sense because there isn't any investment that works this way. And yet, I said I wanted to proceed with these transactions.

I say, no, that's not true. I had nothing from the bank, and I do not have anything from the Ombudsman. I've got no written information from the Ombudsman, when it went to the Ombudsman, other than what CEL sent to me. I've actually contacted another legal team about this and just asked and they're not convinced that the Ombudsman actually dealt with this properly.

I have nothing verbally or in writing from the bank to say they were sceptical. Absolutely not.

…

Asked whether I am suggesting that the FSO report is incorrect, I say, yes, because I've spoken to the bank since that FSO report, but that's between me and the bank. I did not know that I was being scammed until the police came around to my house concerned that all this money was going out and then, they reported it to Cyber Crime; Cyber Crime came round. I was still absolutely convinced this was genuine. We were about to conclude the last transaction. And they said to me, 'Listen, if you put it in, you won't see it. It's definitely a scam.'

Asked when the cyber police came to me and sat me down for that conversation that I have just mentioned, I say that that was sometime in August.

Also, that I just said that this was prior to the last transaction that occurred, I say, no, I didn't make the last transaction. It was after all the transactions have been made that the normal police came round and then, the Cyber Crime Agency came round a couple of days later. And I said, 'Look, they have asked for this last bit of money and then they will transfer me my funds,' and they said to me, 'They won't because it's a scam.' And then, I said,

'You're sure?' So, he said, 'Just. send them a message saying that we're here and see what happens.' So, I sent them a message and said the Cyber Crime team are here. And that was it.

I confirm that the last transaction was never completed, it was never made.

It is being said that my evidence now is that up until sometime in August 2022, I was still convinced that Royal FX was a legitimate investment. Asked whether this is correct, I say, absolutely.

…

It is being said that in the correspondence exchange, it seems that I indicated that I was transferring funds so that I was putting funds into my crypto wallet and then moving it to an external wallet because of blockchain liquidity; and that I also borrowed funds and I also took a loan and took company money for this blockchain liquidity.

Asked whether it is correct to say that in actual fact the reference to blockchain liquidity is a normal action whenever dealing with crypto and blockchain and in the sense that it is not something that would raise any red flags if I just mentioned blockchain liquidity. Asked whether I was aware of that fact, I say that I have no idea. I mean, I've learned a lot since this has all happened. I go back to the beginning; when I come to Royal FX, they wanted me to do the training. I said I wasn't interested. They do it.

Asked when this was mentioned, the liquidity, whether I checked on what it actually was, how it actually works, I say that I looked up blockchain, I looked at liquidity, I looked at their anti-money laundering …

Asked whether I checked personally or I asked an advisor since I borrowed money and did quite a lot of investments from other people's money, etcetera, I say that I googled myself this anti money laundering thing from blockchain and it does appear that you have to put 25% liquidity in. I didn't fully understand it. I still don't fully understand it. But it all tied in with the way the Royal FX were manipulating me. It was all half-truths, if you like, but for somebody that doesn't understand it, it all seemed legitimate.

> *In fact, I actually said to my wife, 'We, have made £300,000 according to them.' I said, 'My God, if we made £1,000,000, we'd have to find £250,000 to put into liquidity to get the money out'.' And that's as far as I went with it. But I really, I still don't understand it today."*[47]

A representative for the Service Provider, *inter alia* submitted:

> *"…we would highlight that the activity related to the service provider occurred strictly from a very narrow time period. We have previously highlighted this in the evidence already, but for the sake of the minutes that we have, the financial activity that is concerning the service provider is restricted to a period from the 25th of January 2022 to the very last transaction on the 22nd of June.*
>
> *Now there has in this case only been one withdrawal address in question, and it's a wallet address which is a Bitcoin wallet. It starts with 3lcSrb and ends in Gsad8. This wallet is not one that is hosted by Crypto.com. And from what we can see, the only transactions that this wallet has had with a Crypto.com Wallet directly originates from (Complainant)'s account.*
>
> *… the transaction monitoring did not trigger any warnings for these transactions. Now the evidence that we have on our side is that there were no such warnings because these wallets merely transacted with Complainant himself, save for some withdrawals and other transactions that they made. In terms of funds received, they only received funds from (Complainant)'s Crypto.com wallet.*
>
> *So, it's not surprising that no warnings were triggered on our end or of that of our service providers. Now, as a financial institution with the licences that we have, our duty is to ensure that the source of funds that we receive are clean and proper; and it was to that extent that we carried out the various processes that we carried out for (Complainant). For instance, he was asked about the source of funds, he was asked about the documentation related to some of his loans, he was asked about documentation relating to his pension, I believe, as well as his windfall from an inheritance he had or was*

[47] P. 457 - 461

due to receive. Those questions are obtained by us and requested by us to ensure that the source of funds is proper and justifiable.

That is what our responsibility is in this case. We carry out Know Your Customer verification of (Complainant). We carry out source of funds analysis of (Complainant) and we also ensure that the transactions that he is about to perform are for a purpose that do not offend anti money laundering or counter terrorism financing - what we call AMLCTF. We do not carry out any further analysis of the purpose of his investments or who he's invested with.

It has been made repeatedly a point after the case, almost three years after the case, that we were warned that he was transacting with his platform called Royal FX. Even on the evidence provided and the FCA's own warnings, Royal FX, in the way that it is spelt and the way that it is stylised, did not pop up as a warning or a warning institution until August of 2023 by the FCA. That's not withstanding the fact that this institution, Foris DAX MT, does not have any direct link with the FCA and, of course, as you all know, we are authorised by the Maltese authorities.

We were in receipt of no warnings; our transaction monitoring triggered no warnings. (Complainant) himself was seemingly oblivious to his own unfortunate situation and, in fact, was carrying out transactions or wanted to carry out transactions on his own, passed his last transaction with us. And we will put it to Mr Arbiter that our responsibilities have been carried out in so far that these transactions are concerned in how we carried out Know Your Customer analysis of our customer, (the Complainant). We verified the source of funds repeatedly on various occasions for various amounts and (Complainant) himself was anxious to push through these transactions, showing the fact that he was not impeded by any other warnings.

So, it is to that effect, that we say that we don't have this alleged duty of care. The extent that we did, it has been discharged and most importantly, the legal obligations that surrounded our institution at the time, which will be different as MICA[48] comes in, was that we only have to ensure that our

[48] MiCA stands for Markets in Crypto Assets Regulation.

customers' funds are proper and clear. So that is what we did in the situation. That is what we've been doing for a number of years.

And on that basis, there should be completely no case found against us …"[49]

The Service Provider's lawyer asked the representative whether he could explain whether there was anything which could be seen out of character to which the representative replied:

"*What we generally do in circumstances like these is that when we see a large transfer come in, we'd like to ascertain where those monies have come from.*

… we could see that (Complainant) self-financed his Crypto.com account with fiat to purchase cryptocurrency. We then checked with (Complainant), notwithstanding that these came from his own named account what the source of that money was, how he came to obtain this money ….

There is a number of occasions where we were not satisfied with the answers and we asked for paperwork and, like I said, all this is in pursuit of the source of funds. ….

… we have obligations to monitor transactions as they occur for the purposes I've mentioned: source of funds, anti-money laundering and counter terrorism financing …

… in this case, the large amounts that (Complainant) was bringing to this account required us to ask him questions as to how he obtained this money. And that the money he was using was for purposes which were not related to counter terrorism funding or anti-money laundering. So that is what I can say about that."[50]

Under cross-examination, the Service Provider's representative further answered:

"*… It is being said that in my explanation of what I was doing, I said that the complainant did not take any note of any warnings from us.*

[49] P. 461 - 463
[50] P. 463 - 464

Asked what warnings we sent to the Complainant, I say that the warnings we sent to the Complainant with regards to his source of funds indicate that a large transaction is about to happen. We asked him for the source of his funds because we wanted to understand where these funds came from knowing that these transactions are apparently outside of his immediate means.

It is being said that I didn't send that as a warning. I just asked for the information, so I have never sent him a warning.

Also, I am being asked what we do with the sheets of paper that he filled in (in his very first interaction with us) with his name, address, etcetera, etcetera. And then it says how much do you intend to use, to put in per month into the wallet in which he put £100 a month which is what he was going to use.

Asked whether we use this information at all, I say that is precisely what triggers our request to the complainant for source of funding. That is precisely why we go to the Complainant to ask and to track the transactions which are about to occur as well as his indications and how they do not fit with the transactions which he was about to perform.

So, with respect to the first of those questions, I believe that was sometime in April of 2022, the Complainant was asked to provide us with information in addition to what he provided us at the account opening; to ask for his source of funds as well as the purposes of his withdrawals, because these were seen to be outside of his regular behaviour as he indicated to us.

It is being said on the same point, that the Complainant thereafter increased his limit from £100,000 a day to £250,000 a day.

I am being asked whether that in addition caused an additional check on our end.

I think the evidence has been filed as regards the correspondence and the number of questionnaires that we had out there. One of the responses we have received from (Complainant), sometime again in April, I believe it's the 19th as well as on the 24th, was that he obtained these amounts through his inheritance. As well as from his personal accounts, some of which were

… So those parameters were adjusted for in light of his declarations of his source of funding. And I can't highlight this enough: what we do is to ensure that the source of his funding is legitimate.

Our obligations are not to scrutinise the transactions that he performs, so long as they are not related to money laundering or counter terrorism financing.

…

Asked when the first date was that we were aware that Royal FX and/or the wallet in particular that the Complainant transferred his money to were involved in any nefarious activity, I say that I do not have that date on hand. We can say that the FCA's alert to us in August of 2023, and the reason why the FCA's alert to us is relevant is because by then, of course, Crypto.com, as a brand, and strictly speaking, Foris DAX UK Limited, which is an affiliate of Foris DAX MT Limited, obtained its Virtual Asset Service Provider licence in summer of 2022. That is why we were in receipt of the FCA's circulars; but that's when the first notification we have of the Royal FX nefarious activities would have come to us.

…

Reference is made to an email of 1st of August 2022, sent by us, in which we informed The Complainant that he may have been involved or transacted with a wallet that was suspicious.

Asked whether I am saying that the 1st of August 2022, when that email was sent, we were aware of their involvement then, and that that was the earliest, I say, no.

I think the 1st of August 2022 and the 4th of August 2023 are quite some time apart. What we do is that whenever there are transactions occurring to non-custodial wallets (which is what we've identified the withdrawal address to be in this case), we do issue generic warnings to our users that they may be implicated in something that might not be toward, but that is different from us identifying Royal FX as a scam platform.

It is being said that, so, the 1st of August 2022 was the warning regarding the activity with a non-custodial wallet which then raised flags on our end.

I say that it did not raise flags on our end, so to speak of. There are very legitimate purposes for why non-custodial wallets are used. I use non-custodial wallets all the time because I prefer to custodize my own funds instead of having a centralised platform. And that's particularly in the light of 2022 and the events of 2022 such as the FTX collapse, 3AC, Three Arrows and Genesis Capital. So, at that point in time, we did issue warnings to users who were transacting with non-custodial wallets. It is a generic warning. It is sent out to many users on many occasions. It is not necessarily something specific to (Complainant) other than the fact that he transacted with non-custodial wallet.

Asked whether we did not think it important to make it specific, or perhaps linked to people who transact with these decentralised wallets to give them warnings of large transactions with those wallets, I say that is precisely what (Complainant) received.

It is being said that it was months after his last transaction and certainly several months after his first.

Asked if we felt that the warning was necessary to people who were transacting with these decentralised wallets (and plainly that's what we thought because the warning was sent), why our firm waited until the 1st of August to do so when it was several months after (Complainant) actually had transacted with that wallet, I say that we issue these warnings to people who come to us complaining of fraud.

Now, the primary reason for that is because when they come to us worried about fraud or having, potentially, engaged with fraudulent situations, what we do is we issue responses to warn them and let them know how they may carry out the filings with the local enforcement.

If you read that generic warning, you will see that what we have told him is that, upon regular reviews of our platform and our users, we found that they may have conducted crypto transactions with wallets linked to a potential scam. The reason we say that they are linked to a potential scam

is because we see that these wallets are basically unhosted and non-custodial wallets.

At that point in time, there was an increased level of fraudulent services and investment services; I think there was one called Petero and Torkbot, which were very popular at that time. And that was precisely in the aftermath of a lot of what was happening in and around the industry at that time that scams were starting to emerge in 2022. In the summer of 2022 to be precise.

Asked by the Arbiter whether this general notice which I am referring to was sent after the last payment was made or before, I say that it was sent out after the last payment was made. We carried out a systemic review of our platform and on the 1st of August, more than one of these were issued to users who had previously conducted transactions with non-custodial wallets.

I will also say that these messages are usually sent as triggered responses, meaning that when users mention the word 'scam' in their messages to us, whether or not it is a legitimate complaint of a scam, or whether it is something that they simply refer to as a scam, this is a generic response that is sent out by one of our automatic bot responses. We do use bot responses in our customer service replies to ensure that a fast reply is given. When the word 'scam' is used, this template was one of those which were triggered by the users' mention of the word scam in their communications with us.

Asked whether we think that it is effective to send non-specific warnings to people who have transacted with a decentralised wallet several months after they had transacted with those wallets; and if we do think that that is sufficient, shouldn't that be done more regularly or more frequently, I ask whether he wants my opinion as I am here as a witness of fact and what is asked is an opinion.

Asked how frequently warnings are sent to people corresponding with decentralised wallets or transacting with decentralised wallets, I say that at the time when these transactions occurred, it was not something that was prevalent amongst our platform or something that was happening regularly to the extent of which it happens today. I would say that in terms of

sufficiency, it is dependent on context. And the context of the time was that in the aftermath of the events that occurred in the summer of 2022, when more and more of these transactions were seen to be floating to the surface, we warned our users who came to us asking for whether or not scams had occurred or if scams were occurring …".[51]

Analysis and considerations

Overview of transactions subject of this Complaint

The Complainant made a series of transfers from his Bank in UK (HSBC) to his account on *Crypto.com*, whereby in total around GBP650,000 were transferred over more than 30 transactions,[52] of which:

- 8 transactions were lower than GBP 10,000
- 13 transactions were between GBP 10,000 and below GBP 20,000
- 13 transactions were between GBP 20,000 and GBP 25,000
- 1 transaction was for a higher amount of GBP 130,000.[53]

Tables A to C below provide an overview of all the transactions authorised by the Complainant as explained and indicated in the Service Provider's reply.[54]

Table A lists the deposits in GBP made by the Complainant to his Wallet with *Crypto.com*.

Table B lists the purchase of Bitcoin (BTC) he then made by exchanging GBP to BTC from his Fiat Wallet (or with a personal debit/credit card as indicated).

Table C then lists the subsequent withdrawals ensuing from his wallet where Bitcoin (BTC) was transferred to an external wallet address.

[51] P. 464 - 469
[52] P. 11 – 12 & 183 - 216
[53] Data from Table A below
[54] P. 183 - 216

Table A

	Date	Deposits in GBP	Deposits in Crypto (BTC)
1	25-Jan-22	10,000	
2	25-Jan-22	5	
3	25-Jan-22		0.00274258 (Approx. EUR 88.77)
4	31-Jan-22	5,000	
5	04-Feb-22	7,500	
6	11-Feb-22	7,500	
7	24-Feb-22	16,020.34	
8	25-Feb-22	22,250	
9	01-Mar-22	25,000	
10	02-Mar-22	25,000	
11	10-Mar-22	15,000	
12	10-Mar-22	10,000	
13	13-Mar-22	15,000	
14	15-Mar-22	10,000	
15	16-Mar-22	25,000	
16	17-Mar-22	25,000	
17	26-Apr-22	20,000	
18	28-Apr-22	130,000	
19	28-Apr-22	16,700	
20	29-Apr-22		0.0319448 (Approx. EUR 1,209.48)
21	11-May-22	25,000	
22	12-May-22	25,000	
23	13-May-22	25,000	
24	16-May-22	5,000	
25	16-May-22	20,000	
26	31-May-22	25,000	
27	02-Jun-22	25,000	
28	07-Jun-22	8,000	
29	08-Jun-22	21,000	
30	08-Jun-22	4,000	
31	09-Jun-22	17,000	
32	10-Jun-22	11,400	
33	10-Jun-22	11,260.80	
34	14-Jun-22	10,500	
35	16-Jun-22	10,800	
36	21-Jun-22	13,375	
37	22-Jun-22	9,785	
	Total	**GBP 652,096**	**BTC 0.0346**

Table B

	Date	Fiat money (GBP) paid to purchase Crypto	BTC Purchased
1	25-Jan-22	9,989.89	0.3576616
2	31-Jan-22	5,006.52	0.177
3	04-Feb-22	7,507.31	0.263952
4	11-Feb-22	7,497.04	0.2294
5	24-Feb-22	16,019	0.5952528
6	28-Feb-22	22,255.19	0.7645927
7	01-Mar-22	24,705.08	0.7354
8	02-Mar-22	25,291.02	0.7521338
9	10-Mar-22	25,003.73	0.8219048
10	14-Mar-22	4,537.35 *	0.15
11	14-Mar-22	15,000.05	0.4945404
12	15-Mar-22	9,999.54	0.332
13	17-Mar-22	49,997.19	1.5910563
14	28-Apr-22	149,989.72	4.6399285
15	28-Apr-22	16,697.18	0.517337
16	28-Apr-22	24.03	0.000748
17	11-May-22	24,994.96	0.9476198
18	11-May-22	2.82	0.0001085
19	12-May-22	25,004.41	1.0105
20	13-May-22	24,933.68	0.9836788
21	16-May-22	25,048.61	1.018
22	31-May-22	25,016.63	0.9802
23	02-Jun-22	24,989.42	1.026
24	07-Jun-22	7,999.83	0.3280021
25	07-Jun-22	12.3	0.0005059
26	09-Jun-22	41,972.27	1.6984561
27	10-Jun-22	11,394.14	0.4618485
28	10-Jun-22	27.89	0.0011331
29	10-Jun-22	11,262.85	0.4622823
30	14-Jun-22	10,501.78	0.555
31	16-Jun-22	10,800.73	0.6170694
32	22-Jun-22	13,375.76	0.7902334
33	22-Jun-22	9,785.55	0.5818385
34	**Total**	**GBP 656,643.47**	**BTC 23.8853843**

* Purchase by personal debit/credit card (P.193)

Table C

	Date	Transfer of BTC to external wallet (excl. fees)
1	27-Jan-22	0.35980418
2	31-Jan-22	0.1764
3	04-Feb-22	0.2633572
4	11-Feb-22	0.2288
5	24-Feb-22	0.5946528
6	28-Feb-22	0.7639927
7	01-Mar-22	0.7348
8	02-Mar-22	0.7515338
9	10-Mar-22	0.8213048
10	14-Mar-22	0.6439404
11	15-Mar-22	0.3314
12	17-Mar-22	1.5904563
13	28-Apr-22	4.63932852
14	28-Apr-22	0.517485
15	11-May-22	0.9790731
16	12-May-22	1.0099
17	13-May-22	0.9830788
18	16-May-22	1.0174
19	31-May-22	0.9796
20	02-Jun-22	1.0254
21	07-Jun-22	0.327908
22	09-Jun-22	1.6978561
23	10-Jun-22	0.4623816
24	10-Jun-22	0.4616823
25	14-Jun-22	0.5544
26	16-Jun-22	0.6164694
27	22-Jun-22	0.7896334
28	22-Jun-22	0.5812385
29	**Total**	**BTC 23.9032769**

Summary of key aspects and main submissions

Various claims and extensive submissions were provided by the parties during the proceedings of this case. The Arbiter shall focus on the main pertinent aspects.

The key aspect of this Complaint basically revolves around whether the Complainant is correct in arguing that the Service Provider failed in its duty of care to protect him from falling victim to a scam. The Complainant argued that the Service Provider failed to spot the operation of the scam and had a duty to intervene and warn him that the history of transactions on his account and his activities were signalling suspicion of fraud.

On its part, the Service Provider maintains that once they verified that the transactions were properly authorised by the Complainant, their duty was simply related to ensuring that the money being transferred by the Complainant from his UK bank account was clean and raised no AML/FT suspicions as to the source of such funds.

The Service Provider further argued that they had no obligations to issue any warnings to the client once they had no reason to suspect that the unhosted wallet where BTC were being transferred had any alert or suspicion of fraudulent activity. The Service Provider also pointed out that the Complainant had ignored the warnings provided to him previously by other financial entities regarding the possibility of the scam.

The Arbiter shall next proceed to consider the following key aspects pertinent to the case in question in order to reach his decision on this Complaint:

(1) The regulatory requirements applicable to the Service Provider at the time and whether Foris DAX was subject to the duty of care and fiduciary duty.

(2) The reasons why, if any, the Service Provider was required to intervene and warn the Complainant in the particular case in question, in terms of the applicable duties and obligations.

(3) The Complainant's actions, the prior warnings he ignored, and the relevant context.

(4) The extent of damages arising to the Complainant, if any, from the actions or lack thereof of the Service Provider.

(5) Responsibility for the losses incurred taking into consideration the parties' actions and relevant aspects.

A). *Applicable regulatory framework and other pertinent matters*

i. VFA Framework

At the time of the events giving rise to this Complaint, Foris DAX was the holder of a Class 3 VFAA licence granted by the Malta Financial Services Authority ('MFSA') under the Virtual Financial Assets Act, 2018, Chapter 590 of the Laws of Malta ('VFA Act').

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 was 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'*[55] 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').

The Arbiter shall refer to the said framework in the consideration of this Complaint.

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

ii. AML/CFT Framework

Further to the Prevention of Money Laundering Act (Cap. 373) and Prevention of Money Laundering and Funding of Terrorism Regulations ('PMLFTR'), the Financial Intelligence Analysis Unit (FIAU) issued Implementing Procedures including on the *'Application of Anti-Money Laundering and Countering the Funding of Terrorism Obligations to the Virtual Financial Assets Sector'*.[56] These are *'sector-specific Implementing Procedures [which] complement the Implementing Procedures – Part I [issued by FIAU] and are to be read in conjunction therewith'*.[57] Section 2.3 of these Implementing Procedures detail the monitoring and transaction records obligations of VFA licensed entities.

It is noted that the VFA Act mainly imposes transaction monitoring obligations on the Service Provider for the proper execution of their duties for Anti Money Laundering ('AML') and Combating of Financing of Terrorism ('CFT') obligations in terms of the local AML and CFT legislative framework.

Failures of the Service Provider in respect of AML/CFT are not in the remit of the OAFS and should be addressed to the FIAU. In the course of these procedures, no such failure was indeed alleged, and the many enquiries made during the course of the relationship to seek clarity about the source of funds being transferred support the Service Provider's adherence with the obligations applicable regarding the verification of the source of funds. The Arbiter shall accordingly not consider compliance or otherwise with AML/CFT obligations in this case.

iii. MiCA and the Travel Rule

As to the identification of the recipient of the funds, it is noted that the Service Provider correctly maintains that MiCA[58] and Travel Rule[59] obligations which

[56] https://fiaumalta.org/app/uploads/2020/09/20200918_IPsII_VFAs.pdf
[57] Page 6 of the FIAU's Implementing Procedures on the *'Application of Anti-Money Laundering and Countering the Funding of Terrorism Obligations to the Virtual Financial Assets Sector'*
[58] EU Directive 2023/1114 on markets in crypto assets https://eur-lex.europa.eu/legal-content/EN/AUTO/?uri=celex:32023R1114
[59] EU Directive 2023/1113 https://eur-lex.europa.eu/legal-content/AUTO/?uri=CELEX:32023R1113&qid=1740401464257&rid=1 and EBA Guidelines on Travel Rule https://www.eba.europa.eu/sites/default/files/2024-07/6de6e9b9-0ed9-49cd-985d-c0834b5b4356/Travel%20Rule%20Guidelines.pdf

entered into force in 2025 and which give more protection to consumers by having more transparency of the owners of the recipient wallets were not applicable at the time of the events covered in this Complaint which happened in 2022. The Arbiter shall thus not consider the MiCA provisions and Travel Rule obligations for the purposes of this Complaint.

iv. Other - Technical Note

A Technical Note (issued in 2025) with guidance on complaints related to pig butchering was recently published by the Arbiter. This Technical Note was referred to and reproduced as part of the Complainant's final submissions.[60] In respect of VFA licencees the Technical Note states as follows:

> *"Virtual Financial Assets Service Providers (VASPs)*
>
> *VASPs should be aware that with the coming into force of Regulation (EU) 2023/1113 and the Travel Rule Guidelines[61] their obligation to have reliable records on the owners of external (unhosted) wallets increases exponentially as from 30 December 2024.*
>
> *Arguments that they have no means of knowing who are the owners of external wallets which have been whitelisted for payments by their client will lose their force.*
>
> *VASPs have been long encouraged by the Office of the Arbiter (in decisions dating back from 2022),[62] for the devise of enhanced mechanisms to mitigate the occurrence of customers falling victims to such scams.*
>
> *Furthermore, in the Arbiter's decisions of recent months there is a recommendation that VASPs should enhance their on-boarding processes where retail customers are concerned warning them that custodial wallets may be used by scammers promoting get-rich-quick schemes as a route to*

[60] P. 474 & 485 - 503

[61] *Guidelines on information requirements in relation to transfers of funds and certain crypto-assets transfers under Regulation (EU) 2023/1113* - EBA/GL/2024/11 of 04/07/2024
https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32023R1113
https://www.eba.europa.eu/publications-and-media/press-releases/eba-issues-travel-rule-guidance-tackle-money-laundering-and-terrorist-financing-transfers-funds-and

[62] Such as Case ASF 158/2021

empty the bank accounts of retail customers and disappear such funds in the complex web of blockchain anonymous transactions.[63]

***Compliance with such recommendations or lack thereof will be taken into consideration in future complaint adjudications**."*[64]

The Arbiter will not apply the provisions of the Technical Notes retroactively. **Hence, for the avoidance of any doubt, the said Technical Note is not applicable to the case in question**.

v. Duty of Care and Fiduciary Obligations

It is noted that Article 27 of the VFA Act states:

"27. (1) Licence holders shall act honestly, fairly and professionally and shall comply with the requirements laid down in this Act and any regulations made and rules issued thereunder, as well as with other legal and regulatory requirements as may be applicable.

***(2) A licence holder shall be subject to fiduciary obligations as established in the Civil Code (CAP 16) in so far as applicable**."*[65]

Article 1124A (1)(a) of the Civil Code (Chapter 16 of the Laws of Malta), in turn further provides the following:

"1124A. (1) ***Fiduciary obligations arise in virtue of law, contract, quasi-contract****, unilateral declarations including wills, trusts,* ***assumption of office or behaviour whenever a person*** *(the ''fiduciary'') –*

(a) ***owes a duty to protect the interests of another person and it shall be presumed that such an obligation where a fiduciary acts in or occupies a position of trust is in favour of another person****; …"*[66]

[63] Such as Case ASF 069/2024
[64] Emphasis added by the Arbiter
[65] Emphasis added by the Arbiter
[66] Emphasis added by the Arbiter

It is further to be pointed out that one of the High-Level Principles outlined in Section 2, Title 1 *'General Scope and High Level Principles'* Chapter 3, Virtual Financial Assets Rules for VFA Service Providers of the VFA Rulebook, that applied to the Service Provider at the time of the disputed transactions in 2022, provides that:

> *"R3-1.2.1 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."*

It is also noted that Legal Notice 357 of 2018, Virtual Financial Assets Regulations, 2018 issued under the VFA Act, furthermore, outlined various provisions relevant and applicable to the Service Provider at the time. Article 14 (1) and (7) of the said Regulations, in particular, which dealt with the *'Functions and duties of the subject person'* provided the following:

> *"14. (1) A subject person having the control of assets belonging to a client shall safeguard such assets and the interest of the client therein.*
>
> *…*
>
> *(7) The subject person shall make appropriate arrangements for the protection of clients' assets held under control and shall ensure that such assets are placed under adequate systems to safeguard such assets from damage, misappropriation or other loss and which permit the delivery of such assets only in accordance with the terms and conditions of the agreement entered into with the client."*

As inferred in its final submissions, the Service Provider seems to contest the existence of a duty of care applicable to its activities beyond its AML/CFT obligations.[67] **This view is not shared by the Arbiter in all circusmtances**.

The Arbiter is of the view that for the general fiduciary obligations to apply in the context of the VFA ACT, there must be something which is truly out of the ordinary and which should really act in a conspicuous manner as an out of norm transaction which triggers the application of such general fiduciary duties.

[67] P. 504

The duty to protect and safeguard assets and interests of the client needs to be seen in the wider context and not just limited to measures to prevent unauthorised access. Consideration needs to be taken of the Service Provider's position vis-à-vis its customer and interplay and relevance of the various provisions quoted including other provisions relating to the PMLFTR framework and the Service Provider's own terms and conditions as shall be considered further on in this decision below.

The Arbiter thus considers that the Service Provider did have, in terms of the provisions outlined in this decision, a duty of care and fiduciary obligations towards its customer, the Complainant, when considering certain particular aspects as shall be delved further in this decision.

Any argument, that given the particular circumstances of this case, fiduciary duties as provided by the Civil Code apply given that Article 27 of the VFA Act is applicable only for the purpose of AML/CFT, is not considered by the Arbiter as a valid argument.

The Arbiter is of the view that general fiduciary obligations in the context of the VFA Act apply in a wider context particularly in situations which are truly out of the ordinary and stand out in a conspicuous manner or which raise reasonable suspicion of fraud or criminal intent and which accordingly trigger the application of such general fiduciary duties where appropriate intervention is necessary to uphold such duties.

B) *Duty and need to intervene*

A key issue which needs to be considered in this Complaint is whether the Service Provider had, in the Complainant's case, a duty to intervene given the suspicion of fraud that the Complainant claimed to have been displayed in his account activity. The Complainant pointed out that he had specifically notified *Crypto.com* on various occasions about his dealings where he specifically mentioned RoyalFX.[68]

[68] E.g. During the hearing of 7 October 2024, the Complainant testified inter alia that '*Obviously, I have given several points of notice here on the platform I am engaging with, which was Royal FX'* - P. 268

i. Claimed lack of due diligence by *Crypto.com* about RoyalFX

The Complainant claimed that RoyalFX was known to *Crypto.com* as it was claimed this was a client of the Service Provider.

It has not been demonstrated nor emerged, however, that the alleged fraudster to whom the payment was made by 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 actually transferring his crypto assets. Furthermore, the Complainant must have himself 'whitelisted' the address giving an all-clear signal for the transfer to be executed.

Complainant's allegation that the '*beneficiary wallet (was) being hosted on the Crypto.com platform'*[69] has been emphatically denied by the Service Provider and has not been proven. *Crypto.com* alleged affirmative reply to Complainant's question whether the beneficiary wallet address was valid[70] does not equate to a confirmation that the wallet was hosted on *Crypto.com*.

The Service Provider was accordingly not bound to make due diligence on RoyalFX in the absence of any client relationship between RoyalFX and Foris DAX. Moreover, **due diligence on the trading platform used by the Complainant to carry out his trades was the responsibility of the Complainant and not an obligation of Foris DAX**.

Another aspect that was raised is that the Service Provider should have undertaken certain checks on RoyalFX (which was mentioned to it multiple times by the Complainant during the communications that the Complainant had with *Crypto.com*). It was claimed that such checks should have been part of the AML/CFT checks given that the Service Provider was aware that RoyalFX was the recipient of the *'staggering amount'* of funds that was deposited to the same wallet address by the Complainant.[71]

[69] P. 3
[70] P. 275
[71] P. 13

Whilst certain checks could possibly have been undertaken in such circumstances, the Service Provider cannot reasonably be expected to have carried out a comprehensive due diligence on RoyalFX.

The obligation for VFAs to identify the beneficial owners of unhosted wallets was not part of the regulatory regime at the time of events that gave rise to this complaint. VFAs obligations of due diligence relate to their own customers, in this case, the Complainant, not to owners of the unhosted wallets recipients of crypto assets transferred by their client.

Obligations for VFA's to identify such beneficiaries only entered into force in 2025 in terms of **EU REGULATION 2023/1113 of 31 May 2023 on information accompanying transfer of funds and certain crypto assets** as further explained in the **EBA Guidelines on information requirements in relation to transfers of funds and certain crypto-assets transfer under Regulation EU 2023/1113 (Travel Rule Guidelines – reference EBA/GL/2024/11 of 04/07/2024).**[72]

Without entering into the merits of whether the Service Provider complied with AML/CFT requirements, the Arbiter rather takes cognisance of the applicable provisions with respect to the Complainant as its customer. For example, section 4.4 of the FIAU's Implementing Procedures Part I provides:

> *"In terms of Regulation 7(1)(c) of the PMLFTR, subject persons are required to assess and, where appropriate, obtain information and/or documentation on the purpose and intended nature of the business relationship. In addition, subject persons are also required to establish the customer's business and risk profile. These requirements entail gathering and analysing information to:*
>
> *(a) determine whether a service and/or product being provided makes sense in the customer's situation and profile;*
>
> *…*
>
> *(e) carry out meaningful, ongoing monitoring since it will be able to understand and identify the expected behaviour, including the expected*

[72] In particular, article 4.8 para 76 – 90. https://www.eba.europa.eu/sites/default/files/2024-07/6de6e9b9-0ed9-49cd-985d-c0834b5b4356/Travel%20Rule%20Guidelines.pdf

nature of transactions or activities, of the customer throughout the business relationship.

4.4.1 Purpose and Intended Nature of the Business Relationship

Subject persons have to understand why a customer is requesting its services and/or products and how those services and/or products are expected to be used in the course of the business relationship".

…

In all cases, subject persons should have a good understanding of how the business relationship will be used so as to carry out proper monitoring, as well as to be able to determine that the product or service requested makes sense in view of the customer's profile …".[73]

The above provides some further context on the nature of the assessment required to be done in respect of the customer. Such a background is more relevant to the case in hand.

ii. Claimed warning about RoyalFX

In his submissions, the Complainant also claimed that *Crypto.com* should have known about adverse information involving RoyalFX, given the warning issued by the FCA, UK.

The Arbiter notes that, as emerging during the hearing of 4 February 2025, there was a warning about the lack of authorisation held by RoyalFX to operate in the UK, with such warning issued by the FCA, UK in August 2023.[74] This notice is, however, post the date of the disputed transactions and, for this reason, not considered by the Arbiter to be relevant for the purposes of this Complaint.

In its final submissions, the Complainant's representatives referred to a similar warning issued by the FCA on 25 June 2020 about *"RoyalsFX"*.[75]

The Arbiter, however, notes that apart from the fact that the warning of June 2020 is about an entity with a slightly different name ('*RoyalsFX*' as compared to

[73] Page 133/134 of the FIAU's Implementing Procedures – Part I (Version: First Issued on 20 May 2021 & Last amended on 18 Oct 2021).
[74] P. 464 – 466; https://www.fca.org.uk/news/warnings/royalfx
[75] P. 481; https://www.fca.org.uk/news/warnings/royalsfx

'RoyalFX', the latter being the only name indicated by the Complainant during communications with *Crypto.com*)[76] the address indicated for 'RoyalsFX' in the FCA's notice of June 2020 was one in Switzerland.[77] This location does not reflect the one with whom the Complainant was dealing with - that is, RoyalFX based in St Vincent & The Grenadines. Neither did the websites listed for RoyalFX and RoyalsFX match.[78]

For these reasons, **the Arbiter cannot give any weighting to such notices both of which are not considered relevant to the case in question**.

iii. Powers of intervention

The Service Provider is considered to have had the power to intervene. It is noted that, as outlined in one of the communications sent by Crypto.com:

> *'In our terms you have accepted during the registration process, it says:*
>
> *…*
>
> *15.1 Crypto.com may at any time and without liability to, terminate, suspend, or limit your use of the Crypto.com Wallet App Services (including freezing the Digital Assets in your account or closing your Digital Asset Wallet, refusing to process any transaction, or wholly or partially reversing any transactions that you have effected), including (but not limited to): (a) in the event of any breach by you of these Terms and all other applicable terms; (b)* ***for the purposes of complying with Applicable Laws****; (c)* ***where Crypto.com suspects that a transaction effected by you is potentially connected to any unlawful activities (including but not limited to money laundering, terrorism financing and fraudulent activities)****;…'*[79]
>
> Whether the Service Provider had not just the power but also the obligation to intervene in a timely manner with some sort of warning about suspicions indications of fraud is considered further in this decision.

[76] E.g. P. 475

[77] https://www.fca.org.uk/news/warnings/royalsfx

[78] In the communication sent by Charles Stanley to the Complainant, reference was made to the URL of RoyalFX being *'www.theroyalfx.io'* where '*The Contact Us page says the registered address is St Vincent and the Grenadines…'* (P. 152). The website is different to the one *'https://royalsfx.co'* indicated in the FCA's notice of June 2020, where the address of RoyalsFX was indicated to be in Switzerland.

[79] P. 392 – Emphasis and underline added by the Arbiter

iv. The extent/size of the transactions

The Complainant referred to the multiple transactions and the size and extent thereof undertaken between January and June 2022.

In the context of the history of the transactions on this account, it is noted that the Service Provider intervened on various occasions to enquire and ask the Complainant about his source of funds and activities. A particular instance which gave rise to such obligation was the transfer of GBP £130,000 effected on the 26 April 2022 (received by Foris DAX on 28 April 2022) together with an earlier transfer of GBP £20,000 on the same day (received on 26 April 2022). On 28 April 2022, these payments of GBP £150,000 were converted to BTC and transferred out to the 'usual' wallet.

This transfer was completely out of line from previous and subsequent transfers which never individually exceeded GBP £25,000. It is evident that Foris DAX made enquiries to ascertain the clean provenance of the funds in question but never indicated any suspicion of fraud even though the conversation from 19 April 2022 till execution of transfer on 28 April 2022[80] should have given rise to such suspicion. The Arbiter notes that there were further other instances where the Service Provider intervened about the source of funds where such suspicion of a scam could have arisen.

The Service Provider indeed intervened to enquire about the source of funds and activities on various occasions including:

a) During March 2022 – In his message with the scammer of 18 March 2022, the Complainant noted that *'Having to give crypto.com lady 6 months bank statements'*.[81]

b) 19 April 2022 – *Crypto.com* requested additional information to conclude *"routine review"*, including copy of the *"inheritance will", "bank statement2*, *"screenshots from the external wallets where you withdraw your cryptocurrency"*.[82] By the time of this enquiry, the Complainant had

[80] P. 363 - 370
[81] P. 168
[82] P. 363

already done GBP 218,275 in deposits (from 25 January 2022 to 17 March 2022) with *Crypto.com* as per Table A above.

c) 22 April 2022 – Requested clarification from the Complainant on what was *"the reason to state an inheritance as a source of funds if is not due for some months"*; for the Complainant to *"elaborate what was the origin of the funds you used for the fiat deposits made to your Crypto.com … account"*; requested again *"screenshots from the external wallets where you withdraw your cryptocurrency"*.[83]

d) 26 April 2022 – *Crypto.com* requested clarification of certain transactions (transfer ins) featuring on his bank statements. It again requested *"screenshots from the external wallets where you withdraw your BTC, once withdrawn from your Crypto.com … wallet".*[84]

e) 29 April 2022 – *Crypto.com* asked the Complainant for additional information, namely: *2A bank statement for the last two months with full transaction history …"*; for the Complainant to *"elaborate on the flow of your BTC withdrawals once withdrawn from your Crypto.com … account"*.[85] By this time the Complainant had already done GBP 384,975 in deposits (from 25 January 2022 to 28 April 2022) with *Crypto.com* as per Table A above.

f) 12 May 2022 – *Crypto.com* requested the Complainant to provide *"clarification about the nature"* of a number of incoming transfers that were *"visible on the provided bank statements"* which included a transfer of GBP 130,000.[86] Again asked the Complainant *to "please elaborate on the flow of your BTC withdrawals once withdrawn from your Crypto.com account"*.[87]

g) 17 June 2022 – Customer support team of *Crypto.com* again contacted the Complainant as they *"need a bit more information from you"*, where they requested him to provide: *"Loan agreements with your friends or business*

[83] P. 368
[84] P. 375
[85] P. 382
[86] P. 386
[87] *Ibid.*

loans to support your recent transactions between 28 April and 06 June 2022"; to *"confirm the external BTC wallet address … where you withdrew all the fund";* and again noted that *"As we previously asked, please elaborate on the flow of your BTC withdrawals once withdrawn from your Crypto.com account as there are no transactions present on the account … showing funds processed back to your account"*.[88] By this time the Complainant had done GBP 628,936 in deposits (from 25 January 2022 to 16 June 2022) with *Crypto.com* as per Table A above.

h) 1 August 2022 – A few days after the Complainant informed *Crypto.com* on 23 June 2022, that he was *"having problems with TheRoyalFx who take money through this wallet"* and asking whether this was a *"genuine trading company"*,[89] *Crypto.com* sent the Complainant a message notifying him *inter alia* that *"… we found that you may have conducted crypto transactions with a wallet address that is linked to a potential scam"*.[90] By the said time the Complainant had done GBP 652,096 in deposits (from 25 January 2022 to 22 June 2022) as per Table A above.

v. Key exchanges and communication by the Complainant with *Crypto.com*

The Complainant provided a timeline of his interactions with the Service Provider which, according to him, had several red flags at different points in time which should have raised suspicion of fraud for someone as experienced as *Crypto.com* with fraudulent activities going on in the crypto world.[91] Obviously, any interactions after the last in the series of transfers complained of, i.e., after 22 June 2022 are irrelevant as once transfers occur on blockchain, they cannot be reversed.

The Arbiter considers the following as the key communications sent by the Complainant to *Crypto.com* in reply to its requests:

a) 19 April 2022 – Complainant explained:

[88] P. 390
[89] P. 394
[90] P. 396
[91] P. 418 - 419

"In reply to your request. The inheritance is from my wife's fathers house and is not due for some months. ***We expect a large input from recent trading with theRoyalfx to come into my wallet from Blockchain****, where I have already sent them the anti money laundering requirement.*

I ***do not expect to put any further trading money*** *into my wallet,* ***only approx £150,000 to show Blockchain liquidity****, Which* ***I have to borrow****, and* ***will be returned as soon as my funds arrive from Blockchain****".*[92]

b) 24 April 2022 – Complainant replied:

"All the ***funds used*** *were from personal accounts and* ***some borrowed from friends****.*

I am ***not sure what you mean by external wallets****. I* ***only have Crypto.com … wallet****. I believe you can see into that."* [93]

c) 27 April 2022 – The Complainant further explained:

"The money from … was a loan from a good friend and has been repaid. The money from … is a loan from my sister in law ... I ***do not have any wallets, the money from Crypto wallet goes only to theRoyalfx****".* [94]

d) 29 April 2022 – Complainant noted:

"Once withdrawn, funds will go into my HSBC bank. I ***have no other wallets****".* [95]

e) 12 May 2022 - Complainant informed *Crypto.com* the following:

"As you are aware, I am ***having to borrow money to provide Blockchain with liquidity****. The 75 k is part of my wife's fathers estate. The* ***140k is from selling my boat****, you will note NYA princess 55 relate to that.* ***Others are transfers and borrowing from my Company, friends and family****.* ***The 100k going in at the moment is from my friends loan****.* ***Once the million plus***

[92] P. 363 – Emphasis added by the Arbiter
[93] P. 368 - Emphasis added by the Arbiter
[94] P. 375 - Emphasis added by the Arbiter
[95] P. 382 - Emphasis added by the Arbiter

goes into my wallet it then goes back to the bank and to repay all my friends. You try raising the sims [sums] Blockchain require and maybe you would understand my problems". [96]

f) 24 May 2022 - Complainant informed *Crypto.com* of the following:

"Hi Guys
I expect next week a large amount into my wallet from Blockchain
I ***would like to transfer it into my bank at £250,000 per day****.*
Can you fix that for me? Regards Alan".[97]

g) 17 June 2022 - The Complainant explained to *Crypto.com*:

"Hi … 1 there are no written agreements between my family and friends. 2 the ***blockchain insisted through HMRC demanding the profit and liquidity returned to TheRoyalFx and sent to my bank****. 3* ***no money is expected to go back to my bank via your wallet, only through TheRoyalFx****.*

You have the only written agreement for £130,000
Hope that answers your questions. If you need anything more please ask".[98]

vi. <u>Identified shortfalls by the Service Provider and lack of intervention</u>

There is no doubt that the Service Provider rightfully intervened multiple times to verify the source of funds throughout the multitude of transactions undertaken by the Complainant over the indicated six-month period.

Whilst intervention was merited and done by the Service Provider specifically with respect to the source of funds, the question however arises whether the replies and information provided (or lack thereof) by the Complainant reasonably necessitated the Service Provider's intervention under their general fiduciary duties (by way of relevant warnings and proper discussion with the client and/or suspension, blocking or limitation of use of his account)

[96] P. 386 - Emphasis added by the Arbiter
[97] P. 379 - Emphasis added by the Arbiter
[98] P. 390 - Emphasis added by the Arbiter

at the time of the multiple reviews and analysis of the Complainant's account and amidst the multiple deposits and transactions the Complainant was making.

The Arbiter considers that sufficient, reasonable grounds and basis exist in the particular circumstances of this case to conclude that the Service Provider failed to adequately intervene. This is when clearly there were various red flags cumulatively piling up throughout the course of operation of the wallet/account. Some of the red flags, individually and even more cumulatively, were evident signs that things were not right, and that appropriate intervention was necessary to safeguard the client's assets and interests.

Apart from the extent of transactions and the high amounts being frequently transacted (which were far from *"a simple withdrawal of cryptocurrency"*,[99] the following factors, especially in their cumulative effect, should have raised concerns:

1) Departure from original intention - In its submissions, the Complainant explained that, at the account opening stage with *Crypto.com,* he had indicated that the intention for the use of the *Crypto.com* services was *"to trade with 'the RoyalFX' for £100 per month"*.[100] This was not disputed by the Service Provider.

   The material divergence from the original intention of investing just a small amount per month was much evident by March 2022 (within just three months), when the sum of £218,275 had already been deposited by the Complainant.

   Despite such volume (with single deposits ranging from GBP 5,000-25,000), the Complainant then approached *Crypto.com* with the intention to make an even much higher one-off deposit of around £150,000.

2) Further discrepancy about the Complainant's intention regarding the extent of his trading – Notwithstanding that in his communication of 19 April 2022, the Complainant indicated that he did not intend to put further

[99] P. 505
[100] P. 475

deposits for trading apart from the additional sum of £150,000, he again materially deviated from such intention. Indeed, not only did he proceed to deposit £150,000 but also kept on making additional high amounts of deposits. On top of the £150,000, he ended up depositing a total additional sum of £267,121 through various multiple incoming deposits undertaken over the subsequent months between May and June 2022, as per Table A above.

3) Expectations of large returns – The Complainant indicated his expectations of receiving high returns from his trades undertaken with another party on various occasions. The communications of 19 April 2022, 12 May 2022 and 24 May 2022 as highlighted above, particularly refer.

4) Financing of deposits through borrowing and sale of assets – It became evident that the large sums of money that the Complainant was investing (in contradiction to his original intentions) were being financed through borrowings, loans and sale of assets. This emerges from the communication of 19 April 2022, 24 April 2022 and 12 May 2022 as highlighted above.

5) Convoluted explanations – It was also apparent that the explanations and answers being provided by the Complainant to the questions raised by the *Crypto.com* support staff, were unclear, convoluted and indicative that the Complainant not really understanding what he was doing.

   He confusingly referred to money needed for *"Blockchain liquidity"*, to *"funds arriv[ing] from Blockchain"*, to *"borrow money to provide Blockchain with liquidity"* that he was *"try[ing] raising the s[u]ms Blockchain require"* and the *"problems"* he was having in this regard, as well as that *"blockchain insisted through HMRC demanding the profit and liquidity returned to TheRoyalFX"* as indicated in his communications above. **His emails of 19 April and 12 May 2022, are particularly telling of the senseless explanations being provided by the Complainant**.[101]

[101] Blockchain itself is namely a record-keeping system (serving as a decentralized ledger to record transactions. E.g. Blockchain is defined on Investopedia as: *"a decentralized digital ledger that securely stores records across a network of computers in a way that is transparent, immutable, and resistant to tampering. Each "block" contains data, and blocks are linked in a chronological 'chain.'"* - https://www.investopedia.com/terms/b/blockchain.asp

6) No external wallets/all dealings revolving a single party/unhosted wallet – The Complainant informed *Crypto.com* on multiple times that the only wallet he had was with *Crypto.com*. His messages of 24 April 2022, 20 April 2022 and 17 June 2022 refer. It was amply clear that the Complainant was transferring all his funds to the same party, RoyalFX, with whom he had indicated he was trading, and that the Complainant was not understanding what the *Crypto.com* support staff had asked of him to explain regarding the flow of his BTC withdrawals undertaken from his *Crypto.com* account, an important aspect related to what was going on.

   No warnings were issued, and the normal operation of the account continued despite that *Crypto.com* had asked for explanations about what was happening once BTC were being withdrawn from his *Crypto.com* account not less than on six different occasions - 19 April 2022, 22 April 2022, 26 April 2022, 29 April 2022, 12 May 2022 and 17 June 2022.

The Arbiter does not accept that *"there was no reasonable basis to suspect such fraud at the material time"*,[102] as submitted by the Service Provider.

Adequate and timely intervention was evidently required to inform Complainant about suspicions of fraudulent activity emerging on his account.

The Arbiter further notes and takes into account also the following in the particular situation:

- Late generic warning – It is noted that the warning of 1 August 2022,[103] came rather late in the day.

  The Complainant had been making a high volume of transactions with the same external wallet over a number of months. Whilst there may be *"very legitimate purposes for why non-custodial wallets are used"*,[104] no warnings were, however, seemingly sent to the Complainant regarding the potential dangers and the need to exercise caution and ensure the identity with whom one is dealing. This despite the extent and amount of transactions that were being executed by the Complainant to the same unhosted wallet.

[102] P. 507
[103] P. 396
[104] P. 467

- Awareness about scams – It is also noted that during the hearing of 4 February 2025, the representative of the Service Provider *inter alia* testified that:

> *"At that point in time, there was an increased level of fraudulent services and investment services. I think there was one called Petero and Torkbot, which were very popular at that time. And that was precisely in the aftermath of a lot of what was happening in and around the industry at that time that scams were starting to emerge in 2022. In the summer of 2022 to be precise".*[105]

The Arbiter, however, observes that pig butchering scams were already evident and reported on in previous periods much earlier than summer 2022. **The Service Provider should have been aware and knowledgeable of pig butchering scams when the disputed transactions occurred**.

Suffice to say that one of the pig butchering cases, which was previously considered by the OAFS (Case 158/2021 against Foris DAX),[106] involved a similar pig butchering scam which occurred in 2021 and of which Foris DAX was aware through a formal complaint way back in 2021.

An FBI Internet Crime Report for 2021 (released in March 2022), specifically highlighted the increase in pig butchering scams.[107]

C) *Complainant's actions, ignored warnings and context*

Having considered the Service Provider's actions, the Arbiter shall next consider the Complainant's own actions as this evidently impacts the decision and extent of any compensation awarded.

The extent of checks done by the Complainant on TheRoyalFX to whom he had entrusted so much money, and about the validity of the requests for additional funds being made by this party, is unclear, but was evidently inappropriate. The

[105] P. 468

[106] https://financialarbiter.org.mt/sites/default/files/oafs/decisions/457/ASF%20158-2021%20-%20AG%20vs%20Foris%20DAX%20MT%20Limited.pdf

[107] https://www.fbi.gov/news/press-releases/fbi-releases-the-internet-crime-complaint-center-2021-internet-crime-report

Complainant was, in the first place, undoubtedly himself responsible for verifying that he was dealing with a suitable party.

It is furthermore noted that, as emerging from the exchanges that the Complainant had with the scammer, the Complainant himself stated on 9 February 2022, that:

> *"I do not have any more cash to put in if that is what you want. It will all have to done with what you have, and if that's not possible then we just sit and wait. If it grows great, if only slowly, still good"*,

And, again, on the 10 February 2022:

> *"… My wife says this is definitely the last input from our funds, anything else will have to come from profits …"*.[108]

Despite the fact that the Complainant had himself stated in early February 2022 that he would not make further investments and transfer any more money, not only did he continue to transfer funds, but the funds he ended up transferring were more than 25 times the sum he had already transferred by then.[109]

Further material aspects that need to be taken into account relate to the warnings and feedback that were given to the Complainant by other third parties as follows:

a) <u>Warning from his pension advisor, *Charles Stanley*</u>:

It is noted that *Charles Stanley* (the Complainant's financial planner involved with his pension) refused to make a payment from the Complainant's pension to RoyalFX when the Complainant tried to get some funds from his pension to transfer to RoyalFX in March 2022.

As emerging from the communications exchanged between the Complainant and the scammer, on 7 March 2022, the Complainant informed the scammer that:

> *"I have been advised by Charles Stanley that they think this is a scam. They will not provide funds and the police have been informed. The*

[108] P. 131 & 132

[109] By 10 February 2022, the Complainant had transferred £22,505. After the said date till 22 June 2022, he ended up transferring £629,591 more.

Royalfx will have to come up with a written contract that this is for real. Have your legal team look at this asap".[110]

The Complainant believed so much that he was dealing with a genuine party that he even stated to the scammer that *"Your company is unregulated in the UK and that does not help. So many scammers out there. Pass it onto Dan and legal"*.[111] The following day, on 8 March 2022, the Complainant even forwarded to the scammer the reply he had received, listing the reasons for the concerns of Charles Stanley's Compliance Department.[112]

Subsequent to this, the Complainant requested the scammer to transfer money back into his bank so that he could *"show to [his] advisor that this is genuine"*.[113] It seems that the scammer managed to convince the Complainant on the 9/10 March 2022, that the transaction was genuine by sending him a payment on a Crypto wallet (instead of his bank account) and providing evidence of the blockchain transfer.[114]

It is noted that a payment of GBP 22,967 was eventually made from the trustees of the Complainant's pension (his Self-Invested Pension Plan, SIPP) on 16 March 2022 as evidenced in the bank statement.[115] It is unclear what has ultimately convinced his pension plan to make a payment or whether this payment was something unrelated to his original enquiry with Charles Stanley.

b) Warnings/feedback from his banker, HSBC: It transpires that the Complainant called HSBC on 9 March 2022 to report a scam[116] – it seems this occurred after Charles Stanley informed him on 7 and 8 March 2022 that they think this was a scam. As detailed in the report of the UK Financial Services Ombudsman ('UK FSO'), the Complainant called again the bank, a day after, on 10 March 2022, to inform it *"that he is satisfied he hasn't been scammed and for the bank to stop any investigation"*.[117] This pairs with the

[110] P. 148
[111] *Ibid.*
[112] P. 151 - 152
[113] P. 153
[114] P. 154 - 155
[115] P. 343 & 375
[116] P. 290
[117] P. 290

exchanges that the Complainant was having with the scammer at the time (and the payment to a crypto wallet referred to earlier above).

It has not been indicated that the Complainant's bank had given him any warnings at that stage in March 2022 (or earlier).

In his attempt to make a payment of GBP130,000 later in April 2022, an intervention was, at that point, made by HSBC as outlined in the UK Financial Services Ombudsman's ('FSO') Report. The FSO report stated as follows:

> *"A later intervention is made on 25 April 2022 for a payment of £130,000, [the Complainant] at first refuses to tell HSBC what he is doing.*
>
> *Once the nature of the payment is discussed, [the Complainant] states that he doesn't understand the logic of why he has to make the payment and that everyone he has spoken to has told him that it doesn't sound right – but yet continues to make the payments anyway which I think was grossly negligent.*
>
> *The call handler on 25 April 2022 says that he is very sceptical and has never heard of an investment working this way and advises that if he chooses to proceed, he will need to take full responsibility for the payment which [the Complainant] agrees to.*
>
> *Overall, given that (Complainant) has ignored warnings from two paid and trusted advisers who are hired to advise on his financial affairs who told him it was a scam, I can't fairly argue that a warning from the bank would have convinced him to stop. He has made a large number of additional payments despite being put on notice that he was being scammed.*
>
> *(Complainant) appears to have been so under the spell of the scammer that he was willing to ignore the advice of both a financial adviser and a pension fund manager. I don't think the bank could have done any more than these two parties had already done to prevent the scam."*[118]

[118] P. 290

In his defence, the Complainant provided some additional information to the OAFS with respect to the FSO's Report, where he *inter alia* explained that:

> *"The calls to the bank to release £130,000, the agent asked where the money was going. I asked him if [he] knew anything about Crypto and he said no, was I sure it was OK to transfer the funds and I said yes. I explained that the money was going to the Royalfx to get the funds out of the Blockchain. He then transferred them.*
>
> *The bank never once stopped any payments ... I only spoke to one person and the bank …"*.[119]

Further to the above, the Arbiter notes that it only emerged that the representative of the Complainant's banker informed the Complainant during a call that he was very skeptical about the investment. During the hearing of 4 February 2025, the Complainant explained:

> *"'Look, I'm not convinced,' and I would make a comment here: the bank never, never once said to me, 'We think this is suspicious.' Not once. I've had nothing from the bank at all. They just asked me, 'You sure you want to invest in this?' 'Yes, I'd like to invest in this.' They didn't say, 'Do you think you should check it out? We think it's suspicious.' If they had thought it was suspicious, they probably would have stopped the payment going …".*[120]

Context

Account is taken of the context within which the disputed transactions have occurred. Apart from the extent of manipulation and sophistication of the scam (as emerging from the exchanges the Complainant had with the scammer), the following factors are also taken into account:

a) *Complainant's mindset with respect to his pension advisor* – In his explanations, the Complainant stated:

[119] P. 292
[120] P. 458

> *"The reason I called my pension provider was because to retrieve my funds from the Royalfx required liquidity into the Blockchain wallet that I assume they had set up …* ***I asked my pension provider if they could do this and they discussed it, but came back saying crypto was out of their expertise****, they had not heard of this, and so would not release any funds. I only spoke to my financial adviser, and as I had done onto the Blockchain site and checked out this liquidity requirement, understood that the pension providers were sceptical of any crypto dealings, and so went elsewhere for the funds"*.[121]

It is also noted that during the hearing of 4 February 2025:

> *"In answer to that, I say that I went to a pension provider to ask for some money to put into this investment company.* ***They have no experience in crypto whatsoever, which they admitted they had no idea of crypto. They would not, as a pension provider, allow me to do anything with crypto, period****. That was the end of the story."* [122]

b) *Mindset with respect to his Bank* – During the proceedings of the case, the Complainant explained:

> *"I did tell the bank after reporting it as a scam by my pension provider.* ***As he had no knowledge of crypto I could see he could say nothing else*** *…".*[123]

During the hearing of 4 February 2025, the Complainant further testified:

> *"So going on from that,* ***the Royal FX said, of course, nobody wants to deal with crypto at the moment because the normal banking is losing millions to crypto investment which seemed reasonable to me****."* [124]

In a message on 26 January 2022, when the Complainant contacted *Crypto.com* Support due to *"My card crypto purchase failed*", the *Crypto.com* Support explained that *"Your most recent attempt for card purchase of cryptocurrency has been declined by your card issuer … The*

[121] P. 292 – Emphasis added by the Arbiter
[122] P. 458 – Emphasis added by the Arbiter
[123] P. 292 – Emphasis added by the Arbiter
[124] P. 458 – Emphasis added by the Arbiter

most common reasons for a card transaction to be declined by the issuers are: - restrictions over a certain type of transactions, like crypto purchases, among others …".[125]

It is further noted that in a message on 23 March 2022 exchanged with the scammer, the Complainant himself stated that *"Banks won't touch crypto"*.[126]

From the early stages of the scam, as early as in February 2022, the scammer had seemingly subtly planted the idea to the Complainant that banks were against cryptocurrency. This was evidently done to downplay any possible warnings and intervention on the bank's part as anticipated by the scammer, in turn making it easier for the scammer to manage any arising concerns and continue with the manipulation of the victim, notwithstanding the bank's intervention, as has happened in this case. When the scammer was enquiring with the Complainant as to the status of the bank transfer and the Complainant messaged him (on 11/02/2022) that *"Looks like fraud have stopped it …",* the scammer in return replied to the Complainant by stating: *"The banks against Crypto so obviously they will refuse …"*.[127]

D). *Impact of lack of proper and merited actions*

The Arbiter considers that there are three pronounced stages at which the Service Provider ought to have intervened on the basis of the replies received from the Complainant to its queries. These are following the queries and replies received on the same day of 19 April 2022, 12 May 2022 and 17 June 2022.

It is noted that any immediate intervention by the Service Provider on or following 19 April 2022, would have been prior to or around the call of 25 April 2022 that the Complainant had with HSBC Bank were the Bank had seemingly first indicated that it was *"very sceptical and has never heard of an investment working this way"* as indicated in the UK FSO's Report.[128]

[125] P. 325
[126] P. 172
[127] P. 134
[128] P. 290

Hence, this would have been a most timely warning at the time which would have also shortly followed the earlier warning provided by Charles Stanley in March 2022.

The ensuing transactions which subsequently occurred (from 26 April 2022, till the next trigger event of 12 May 2022) amounted in total to a cumulative further amount deposited of £191,700 with *Crypto.com* which were transferred to the scammer.

Any interventions by the Service Provider following the replies of 12 May 2022 and 17 June 2022 would have supported and strengthened the warnings previously provided even further.

The Complainant proceeded to make many more transactions. Between 12 May 2022 and 17 June 2022, the Complainant deposited £218,961 and after 17 June 2022 a further £23,160, which he proceeded to convert into BTC and transfer to the scammer (as per Tables A to C above).

The Arbiter notes the context within which the Complainant took his decisions and the mindset which affected his approach to the warning from his pension planner and feedback from his bank as outlined above.

In the circumstances, there is a possibility that **a warning from Crypto.com**, a professional party solely focused in crypto and, thus, an expert in this line of business, could have reinforced the warnings given by other professionals who were however not involved in this line of business.

It is difficult to determine the impact that could have resulted from the Service Provider's issuing due warning about suspicions of fraud. Even if the possibility of the Complainant's heeding an appropriate warning issued to him by the Service Provider is, in the circumstances, considered low, it does not exempt the Service Provider from their obligations.

Furthermore, besides the issue of warnings, the Service Provider had other measures available to it (such as suspension and limitation of use) of the account which could have been applied in addition to a due warning to protect the Complainant's interests and his assets.

E) *Extent of responsibility*

There is no doubt that the Complainant was primarily responsible for the losses he has incurred due to his own actions and negligence considering various factors:

(i) the lack of adequate and proper due diligence about RoyalFX that he evidently did not carry out about this party and the requests being made for additional funds (ii) exceeding his own imposed limitations on the extent of amount to be invested or transferred to this party (iii) providing the scammer access to his computer/applications through the Anydesk app (iv) ignoring the concerns and specific warning provided by his pension planner, Charles Stanley, in March 2022 about the possibility of this being a scam; (v) ignoring the feedback provided by HSBC in April 2022 and the skepticism pointed out to him by the Bank's representative about the investment.

However, the Complainant's actions do not exonerate the Service Provider from its identified shortfalls and failures.

Material difference from other cases

Apart from the differences in the particular circumstances of the case, the Complainant's case stands out from the various other cases decided by the Arbiter against Foris DAX which were not upheld.

A key material difference is the information that has emerged that the Service Provider was in possession of about the activities of the Complainant which included various red flags. This information resulted during the communications that the Service Provider held with the Complainant when reviewing the source of funds at the time of the numerous frequent transactions in high amounts that the Complainant was making during a six-month period.

Once the Service Provider was evidently in possession of information and sight of activities which should have created awareness about the likelihood of fraud or inappropriate behaviour, the Service Provider is considered to have had a fiduciary obligation to intervene at least by issuing a dutiful warning of its suspicions.

Decision

The Arbiter sympathises with the Complainant for the ordeal he suffered as a victim of a scam but, in the particular circumstances of this case, he cannot accept the Complainant's request for compensation.

The Arbiter is, however, of the opinion that the transaction of GBP £130,000 above referred to and other subsequent interventions should have triggered enough suspicion to require the Service Provider not only to question the clean provenance of the funds for AML/CFT purposes, but also to discuss the possibility of fraud with the Complainant and/or take other measures within its powers as outlined above. This view is fortified by the discussion held between the Complainant and a representative of the Service Provider on 19 April 2022, 12 May 2022 and 18 June 2022.

Crypto.com **should have the experience to judge that the situation that prevailed at the time and the Complainant's comments carried the smell of fraud and should have extended in this direction the conversation they were having with the client and intervene appropriately.**

However, the Arbiter is of the opinion that even if the Service Provider would have issued as a minimum due warning according to their fiduciary obligations, it is highly unlikely, given the particular circumstances, that the Complainant would have given heed to such warnings and withheld payments. The Arbiter's view is supported by the fact that the Complainant disregarded warnings from independent competent persons, such as his pension advisers and his UK Bank, and obstinately continued to put his misplaced faith in the fraudsters to the point that the UK Police had practically to force him to withhold the last payment and accept the reality of the scam. He stated:

> ***"And it was only when the Cybercrime Police from my local county actually came to the house and told me it was a scam, that I realized it was a scam. So, up to that point, I was convinced it was a genuine operation."***[129]

Consequently, the Arbiter sees no direct causation between the Service Provider's failure in their fiduciary duties and the losses claimed by the

[129] P. 266

Complainant. The Service Provider's failure is considered as a regulatory issue which should be handled by the Regulator (MFSA)[130] to whom a copy of this decision will be submitted for their consideration.

Accordingly, the Arbiter dismisses the claim for compensation.

Each party is to bear its own legal costs of these proceedings.

Alfred Mifsud
Arbiter for Financial Services

Information Note related to the Arbiter's decision

Right of Appeal

The Arbiter's Decision is legally binding on the parties, subject only to the right of an appeal regulated by article 27 of the Arbiter for Financial Services Act (Cap. 555) ('the Act') to the Court of Appeal (Inferior Jurisdiction), not later than twenty (20) days from the date of notification of the Decision or, in the event of a request for clarification or correction of the Decision requested in terms of article 26(4) of the Act, from the date of notification of such interpretation or clarification or correction as provided for under article 27(3) of the Act.

Any requests for clarification of the award or requests to correct any errors in computation or clerical or typographical or similar errors requested in terms of article 26(4) of the Act, are to be filed with the Arbiter, with a copy to the other party, within fifteen (15) days from notification of the Decision in terms of the said article.

In accordance with established practice, the Arbiter's Decision will be uploaded on the OAFS website on expiration of the period for appeal. Personal details of the Complainant will be anonymised in terms of article 11(1)(f) of the Act.

[130] Malta Financial Services Authority