Before the Arbiter for Financial Services

Case ASF 151/2024

TL

(the 'Complainant')

vs

Foris MT Limited

Reg. No. C 90348

(the 'Service Provider')

Sitting of 10 January 2025

The Arbiter,

Having considered in its entirety the Complaint filed on 25 July 2024, including the attachments filed by the Complainant,[1]

The Complaint

Where, in summary, the Complainant claimed that four unauthorised transactions took place from his Crypto.com Visa Card to the beneficiary "*Zettle*Mbs Autocare L*" on 2 June 2024. The four transactions amounted to a total of (GBP)£650.00.

Once he noticed the said transactions, the Complainant reported them immediately to the Service Provider. However, he claimed that the Service Provider failed to take his complaint seriously and failed to make a chargeback.

Moreover, the Complainant made reference to a Visa Zero Liability policy which guarantees that, as a consumer of the Crypto.com Visa Card, he would not be

[1] Complaint Form from page (p.) 1 – 6 and attachments p. 7 – 14

held responsible for any unauthorised charges made from his account. He argued that Crypto.com did not comply with this policy.

By way of remedy, the Complainant is requesting the recovery of the full sum of £650.00.

The reply of the Service Provider[2]

"*Dear Arbiter,*

With regards to the complaint filed by Mr. TL with the OAFS, kindly find below a full summary of the events, which precede the formal complaint.

Background:

- *Foris MT Limited (the "Company") is a holder of a Financial Institution Licence, and authorized by the Malta Financial Services Authority, located at Triq l-Imdina, Zone 1 Central Business District, Birkirkara, CBD 1010, Malta. Foris MT Limited, a private company incorporated in Malta, with registered addressed at Level 7, Spinola Park, Triq Mikiel Ang Borg, St. Julians SPK 1000, Malta, is the issuer of the Crypto.com Visa Card. The Crypto.com Visa Card is a prepaid card that functions similarly to a debit card. Unlike debit cards, which are directly linked to an individual bank account, the Crypto.com Visa Card is topped up through bank account transfers, other credit or debit cards, or cryptocurrency.*
- *Upon the successful application for a Crypto.com Visa Card and the acceptance of the relevant Terms of Use, Mr. TL (the "Complainant") became a customer of Foris MT Limited on May 10, 2021.*
- *The Company notes that in the submitted complaints file, Mr. TL has outlined his desired remedy as: (i) reimbursement for a total of four individual transactions made with his Crypto.com Visa Card, amounting to £650 (approximately 757.86 EUR).*

Timeline:

[2] P. 19 – 23

27 May, 2024[3] – the Complainant contacted the Crypto.com Customer Service Team, reporting that he does not recognize four transactions made with his Crypto.com Visa Card.

Kindly find information about the above-mentioned transactions here below, as well as a screenshot from our system, appended under the name Fig. 1 in the Appendix at the end of this letter:

Trans. ID	Trans. Date	Trans. Time	Class	Trans. Type	Description	Amount
623228282	06/03/2024	05:36:09	Trans	PurchaseTrans	POS Signature Purchase International using Google, ZETTLE_*MBS AUTOCARE L, LEEDS, GBR	£50
623228280	06/03/2024	05:36:09	Trans	PurchaseTrans	POS Signature Purchase International using Google, ZETTLE_*MBS AUTOCARE L, LEEDS, GBR	£100
623228278	06/03/2024	05:36:09	Trans	PurchaseTrans	POS Signature Purchase International using Google, ZETTLE_*MBS AUTOCARE L, LEEDS, GBR	£50
623228272	06/03/2024	05:36:09	Trans	PurchaseTrans	POS Signature Purchase International using Google, ZETTLE_*MBS AUTOCARE L, LEEDS, GBR	£450

The four disputed transactions in question were escalated for review to the Foris MT Limited Chargebacks team, in accordance with our established internal procedures. Following their review, our Chargebacks Team issued an opinion that, based on the information available, we are unable to honor the user's request for a refund and dispute the afore-mentioned transactions.

To provide additional context for our decision, all four transactions flagged by the Complainant were conducted through the Google Pay payment platform. Mr. TL's Crypto.com Visa Card was added to Google Pay, and to complete this process, approval was required via an SMS or OTP (one-time password) sent to his

[3] This date is evidently incorrect as the disputed transactions were charged on 03 June 2024.

personal mobile device. Without this authorization step, the disputed transactions could not have been executed by the alleged third party.

For your reference, screenshots of our internal escalation and decision process have been included in the Appendix as Fig. 2. Additionally, further screenshots illustrating the Google Pay integration and SMS delivery are provided as Fig. 3.

In summary, after a thorough review of Mr. TL's complaint, the Company is of the opinion that we must uphold our decision to decline the reimbursement request for the four transactions in question. Our investigation revealed that these transactions were conducted through Google Pay, which requires prior authorization via an SMS/OTP confirmation.

The SMS/OTP confirmation was sent to and authorized from the user's personal mobile device, thereby confirming the user's consent and authorization for integrating the card with Google Pay and subsequently approving the transactions.

Given that the transactions were validated through a secure authentication method, we must conclude that they were executed with the account holder's approval. Consequently, we are unable to consider these transactions as unauthorized or fraudulent.

We remain at your disposal for any further information you may require pertaining to the above case."

Hearings

During the first hearing on 8 October 2024, the Complainant submitted that:

"***On the 1 June 2024[4], I noticed an unauthorised access of four transactions made in pounds of £50, £100, £50, and £450. I still do not know to whom they were paid or who took the money. I did not receive any services or goods.***

On the statement there is mentioned 'Zettle Mbs Autocare L' and I still do not know who they are.

[4] This date is evidently incorrect as the disputed transactions were charged on 03 June 2024.

So, as soon as I noticed the unauthorised access, I notified straightaway Foris DAX which is a Crypto.com App Customer Service. I was expecting a chargeback or as a customer, a recovery of my funds which did not happen.

And that is why we are here. Long story short.

As far as I know, there are Visa policies to protect consumers against all these frauds. For me it is strange that as a consumer, I did report this and this was not taken as a serious case. I do not know why because all the procedures were followed correctly."[5]

On cross-examination, the Complainant submitted:

"***Asked whether I used the Google Pay system with my Crypto.com Visa Card, I say, yes. You may have proof of the history of that Visa Card that day that the only transaction that I tried to do was to top up my phone. You may have the history from Google the secure certification from my Eircom which is possibly, as I mentioned, that my phone was hacked. I cannot explain how that happened. I do not know how they end up charging these transactions to me.***

I confirm I had Google Pay installed on my Android Phone.

Asked whether I used the Google Pay linked to my Crypto.com Visa card to pay for things in the past, I say that, yes, I use Google Pay even before these transactions.

Asked each time I use Google Pay, for example, if I made an online payment what notifications would I receive from Google Pay, I say that I cannot answer because that day it was not successful. And that is why I attempted four times using that card but I was not successful. So, I have this history and I cannot explain because my phone was acting strange and I was on hold after confirming the code and still my card wasn't topped up. And I was on hold, I was waiting. And that is why I attempted four times. I even printed the history from Google.

Asked to explain what I meant when I tried to do a transaction four times, I say that the transaction was to top up my Eir card which is my mobile phone card which wasn't successful that day. So, I have another card from Revolut and that

[5] P. 24

day I used the Revolut card to complete my transaction. For me this was strange. I thought that maybe there is some logging on the system or something and I left it like this but then later, when I checked by balance, I found your price (?); these unauthorised transactions for this amount of money.

I tried to make the transaction on 2 June 2024 but I noticed this on 3 June when I did the complaint straightaway as soon as I noticed it.

Yes, that day my phone was acting strange and I used the Revolut card.

Asked regarding the document with notifications that I tried to show during this hearing, what were these notifications, I say that there were no notifications. There was a circle spinning, like loading. No this was not with Google Pay. It was from the site of Eir.com. that wasn't from Google Pay.

Yes, when I was trying to make these four transactions to top up my Eir card, I was getting this spinning.

Asked whether I received notifications from Google Pay or from my OTP, I say, yes, and once I put that on Eir.com it was spinning and the transaction was not successful. That's why I tried for several times. To complete the transaction which was not successful, at the end, I moved on to a different card.

I say, yes, I kept inserting the code every time I needed to refresh.

To clarify, I confirm that every time that I tried to do the transaction with Google Pay using my Crypto.com Visa card, on the website I have to insert a one-time code that Google Pay sends me to make the transaction. So each time that I tried to make the individual transactions, Google Pay would send me a new code and I would have to put that code from my phone and put it into the website to make this transaction.

But each time I inputted this one-time password, the Eir website would just spin and it seemed to me that these transactions never went through.

I say, yes, I reported this fraud to the police. I went to Mullingar station, the local police and I reported this after reporting to Crypto.com.

Asked if this report is still pending, I say that, as far as I know, the last time I was on the phone was with one of the officers about the investigation. Actually, he did contact me. I asked whether there were any updates, whether I got my funds refunded and said that I didn't and since then I did not contact them. I was waiting for this meeting to see what happens after.

I know that they did try to contact you at Crypto.com and when I asked them, they said that their attempt was unsuccessful. I do not know if eventually they got you or not.

It is being said that the 'Mbs Autocare L' company actually exists. It is a registered company in the UK which sells car parts. Asked whether I am aware of this fact, I say that no. I did not get this information when I asked for it. Maybe somebody in the UK made that transaction. An in-depth investigation would possibly detect from which device the transaction was made. I can promise that this was not made from my device. Such an investigation would uncover who ordered and received these parts which were paid from my Visa card. That would be great; if this is a legitimate company, they might be able to provide to whom they sent these parts or provided their services, whatever they do.

I can confirm that it was not me as these days I was in Ireland, so I wasn't even in the UK. So that's another thing; it's even a different country.

I am being referred to what I said that the phone was acting strange around the material date. Asked what do I mean by the phone acting strange, I say that at that time I did not think that it was acting strange but when I saw what happened, when looking back and thinking what possibly happened, that spinning was strange and the transaction never happened. So, for me it was strange that the phone was logged in and I thought it could have been a software issue or something. When you try to make a transaction, usually it goes. It never happened to me before so it was strange.

Asked whether I checked with Eir if there were any breaches in their website at that time, I say that when you top up with the Eir card usually when it's successful, you will receive the message straightaway that the top-up was successful. Here, I did not receive it and the wheel was still spinning. And since it was not successful, I thought that there was an issue with the card. So, that's

why after a while, I took the other card, I used the Revolut and the transaction was successful. And I received a message from Revolut straightaway.

Asked whether I used Google Pay when I used the Revolut card or I inputted the credit card number directly, I say that for the Revolut card, I think I inputted the number but I cannot remember 100%.

I am trying to remember. That day using the Crypto.com card, if I remember correctly now, when I tried to top up, I entered first the details of my card on that Eir site. And then I was asked straightaway and directed to add this card to Google Pay. That kind of thing. And with Revolut, the top-up was successful. It has been some time and I cannot remember in detail if this was done in the same way or a different way but I can confirm with Revolut that the €20 top-up was successful.

I topped up my card with Eir through Eir's website.

Asked by the Arbiter at what point in time was this Crypto.com card loaded on to Google Pay; whether it was loaded at the time that I was trying to make these transactions with Eir or whether it was already loaded and used it through Google Pay before this incident.

As far as I remember, it was used before. Also, I changed the phone and at that time I was trying to pay for the €20 top-up on the website when I entered the details, I was asked again to add it to the Google Pay.

Asked whether it was because I was using a different phone, I say that I upgraded the phone, I got a new phone.

Asked whether this was the first transaction with the new phone, I say, yes.

So, yes, at that point in time, a new one-time password was sent to me to load the Google Pay card onto the Google Pay on the new phone.

Asked by the Arbiter whether I received confirmation of these four payments from Google Pay, I say, no. That is the thing, I did not receive from Google any confirmation like that. I accept there was this change and I did not expect to receive anything from Google straightaway.

The Arbiter states that it gives him the impression that those four payments were made from my old phone and not from my new phone and the confirmations were sent to my old phone.

I say, no. I did not have the old phone because I change the phone. I got the new phone and I kept the same SIM card and I kept the same number.

The only notification I received was through email which I did not check at the time. Only later did I notice the emails that said that I made this payment. But I did not receive from Google that I made £450, £50, £100, and again another £50."[6]

The Arbiter requested the Service Provider to explain whether it is normal for the system to accept four transactions from the same provider at the same time, as these transactions were made in one second.

The Arbiter also asked the Service Provider to clarify whether Visa was actually informed about these transactions in order to start investigations with the Merchant concerned.

During the second hearing on 26 November 2024, the Service Provider submitted:

"***In order to answer the Arbiter's questions and in response to his queries, we have made some inquiries into the transactions in this case, and the Arbiter is right to say that, as per the logged time of the transactions, all these transactions occurred somewhat simultaneously, but we would actually direct the Arbiter to look also at the transaction IDs.***

They are similar, but a number of transactions apart. For instance, the first one for £450 is number 72, the next one for £50 is number 78, the next one for £100 is at 80 and, finally, the last transaction is 82. So, what actually happens in this case is that when transactions happen in quick succession or close together, the transactions are processed in batches. So, what appears to the user is that the transactions happening at the same time is merely a set of transactions that have been grouped together for the ease of processing. So, strictly speaking, these transactions wouldn't have occurred at exactly the same time;

[6] P. 25 – 28

they would have occurred spaced out, however slightly or perhaps minutes apart.

We can see this from the transaction history and the transaction ID. The four transactions are actually spaced out by 10 different transaction numbers, and the evidence on our side is that these transactions were simply batch-processed; raised and happening all at the same time in the same second of the day.

So, in respect to these transactions, we would say that we can see that these were processed using Google Pay. Google Pay requires a user to link their credit cards or their debit cards to the Google Pay system through an SMS code or a one-time passcode. That is to say that the registered user must themselves authorise the tie up between the Google Pay account and the card in question.

The SMS is sent to the registered phone number registered to the card in question. So, if Mr TL hasn't authorised these transactions, he has been negligent in allowing someone else to tie up the card to the Google Pay account because he must himself has also lost authority or control over his registered device.

These transactions are then carried out either through phone or through mobile, or through website. In either case, the Google Pay account is usually logged into, for instance, when it happens on an Android device. There is an unlocking feature or a code that has to be entered before the transactions can be authorised. In the case of a phone with a smartphone feature with the camera, sometimes this is due to face ID. So, what we would say is that in spite of the evidence given by the Complainant, we would say that these transactions are authorised by Mr TL, the Google Pay tie up was authorised by someone entering the matching SMS or one-time passcode which was sent to his registered device. And, as such, it is not for Mr TL to say that he didn't authorise these transactions. We have carried out the usual security features in processing these transactions. We can see that these transactions were processed from a linked Google Pay account. They did not happen at the same time because they were processed in batch, and we will say that there is no basis for Mr TL to request a reversal of these charges on that basis.

Asked by the Arbiter whether I can clarify whether, in spite of everything I said, there was an attempt to start a chargeback procedure, I say that the chargeback procedure would have to be instigated by Mr TL with VISA directly and not through us. From what I can see, we were merely asked to review his transactions on Crypto.com site and Foris MT's side and having performed our internal procedures, we did not accept his request for reimbursement.

Asked by the Arbiter whether we were the card issuer, I say, yes.

Asked why then the client has to go to VISA directly and not through us, I say that we did carry out our internal review of these transactions and he was told of the rejection of the reimbursement request.

The Arbiter would like to clarify whether I am saying that we did not deem it proper to start a chargeback procedure because according to our records, these transactions were properly authorised, I say, yes.

The Arbiter states that the merchant was not in any way involved in this saga, I say that the review we carried out was internal."[7]

On cross-examination, the Service Provider submitted:

"***It is being said that the complainant contacted VISA also and he was told that it's only up to the provider to do the chargeback and escalate the issue, so he did. Asked whether we made the investigation and found who took his money and from which country, I say that when we reviewed these transactions, we saw that they had been properly authorised.***

It is being said that these transactions were even confirmed as payments, not the amount was taken as he believes that his phone was hacked and that he did see different things on his screen confirming this transaction. So, somebody took the money from the Google but not from his device. He states that it was even a different country, probably different currency.

I say that I can't speak to the circumstances that he saw before his eyes when he carried out whatever transactions involved in this circumstance. What we can say is that these transactions on our system were logged carefully and securely through the tie up through Google Pay. Now if the complainant's

[7] P. 29 – 31

Google Pay was hacked, as he said it was, or if his device was hacked, as he said it was, then it's not for Crypto.com to reimburse him for instances of his negligence, and we are absolutely sympathetic to hear that he has suffered from some phishing attack or some phishing scam, but it's not for Crypto.com to reimburse him for those losses which have occurred due to his negligence."[8]

The Complainant states that he is resting his case on the evidence he submitted.

In their final note of submissions,[9] the Service Provider declared:

"*Background:*

1. *Foris MT Limited (the "Respondent"), offers the following services: issuing and servicing of the Crypto.com Prepaid Visa Card (the "Visa Card"). The Visa Card is a prepaid card that functions similarly to a debit card. However, unlike debit cards, which are directly linked to an individual bank account, the Crypto.com Visa Card is topped up through bank account transfers, other credit or debit cards, or cryptocurrency.*

2. *The Complainant became a customer of the Respondent upon successfully applying for a Visa Card on 10 May 2021 and agreeing to the Terms and Conditions.*

3. *The material transactions which the Complainant has identified as being disputed occurred on 3 June 2024 and relate to four transactions charged to his Visa Card (the "Disputed Transactions").*

Issue (1): Gross Negligence

4. *It is not disputed that on 2 June 2024, the Complainant registered his Visa Card with Google Pay on his personal mobile device.*

5. *It is not disputed that on or about 3 June 2024, over the course of four transactions, the Complainant's Visa Card was charged a total of £650. These transactions, the Disputed Transactions, were successfully executed through the Google Pay payment platform.*

[8] P. 31 – 32
[9] P. 35 – 36

6. *After the Disputed Transactions occurred, the Complainant contacted the Crypto.com Customer Service team on 3 June 2024 to report the Disputed Transactions.*

7. *It is submitted that in order for the Disputed Transactions to have been successfully executed, the Complainant would have had to approve each of the transactions via an SMS or OTP (one-time password) sent to his personal mobile device.*

8. *It is the Complainant's evidence that his phone was acting strange on the material day and that he had attempted to use his Visa Card through Google Pay to top up his mobile phone card on the Eir.com website four (4) times. However, each transaction was unsuccessful after the Complainant entered the SMS/OTP code for each attempt.*

9. *The Respondent has no connection with www.eir.com. The Respondent would like to highlight the fact that the Complainant's failed transaction attempts were not conducted through the Crypto.com App but instead through the eir.com website and Google Pay.*

10. *On the basis of the Complainant's oral evidence given on 8 October 2024, the Complainant admits to his phone having been hacked although he cannot explain how that happened.*

11. *As outlined in the Respondent's evidence, the Disputed Transactions appear in the Respondent's records as being logged clearly and executed securely through Google Pay.*

12. *On the balance of the foregoing, while the Complainant seems to have fallen victim to a form of hack or phishing, it is the Respondent's case that the Complainant should be responsible for any losses which occurred out of his own negligence in accordance with Clause 5.6 of the Terms and Conditions.*

<u>Conclusion</u>

13. *In summary, the Respondent would submit that the Disputed Transactions were authorised by the Complainant through either his active participation of providing the SMS/OTP on four (4) occasions or by*

providing someone with access to this information through his gross negligence. The Respondent ultimately bears no responsibility for merely carrying out the Disputed Transactions as instructed through the Complainant's Crypto.com Visa Card."

Consideration and analysis

Having seen the statements and evidence submitted by the Complainant;

Having seen the statements and evidence submitted by the Service Provider;

The Arbiter proceeds to determine and adjudge this Complaint by reference to what, in his opinion, is fair, equitable and reasonable in the particular circumstances and substantive merits of the case.[10]

There is no doubt that for some reason which only the Complainant can explain, the secret credentials which control and authorise transactions via Googlepay on his new mobile phone were, somehow, knowingly or unknowingly, disclosed to third persons who authorised the disputed transactions in a way which could not have been evident to the Service Provider.

Consequently, the Arbiter finds no grounds to fault the Service Provider for refusing to settle the claim of the Complainant.

There is however an issue as to whether the Service Provider, rather than simply refusing to honour the claim through its own internal procedures on the basis that the transactions were properly authorized by the Complainant, should have escalated the chargeback claim to Visa through the latter's chargeback mechanisms.

In case of fraud, which in this case seems quite probable, there is an obligation to do whatever possible to use all mechanisms to prevent recurrence which could involve other innocent consumer victims.

Accordingly, there was a certain logic that the chargeback should have been referred to Visa who could have a wider perspective whether the particular Merchant could have been part of the problem (in case the Merchant themselves could have participated in the fraud) or part of the solution (in case

[10] In terms of Article 19(3)(b) of CAP. 555 of the Laws of Malta

the Merchant could identify or provide information leading to identification of the fraudster).

Decision

For reason above explained, the Arbiter declines this Complaint but orders the Service Provider to activate the elevation of the chargeback procedures to Visa.

If this elevation is still possible with Visa rules time bounds, the Service Provider should keep the Complainant fully informed of chargeback fate.

If this elevation in so no longer possible due to Visa time bounds for raising such chargebacks, then, the Service Provider is ordered to pay moral damages to the Complainant for 50% of the claim, i.e., GBP £325 (three hundred and twenty-five GBP pounds sterling).

The above is in terms of Article 26(4)(c)(iv) of CAP. 555 of the Laws of Malta.

Each party is to bear its own cost of the proceedings.

Alfred Mifsud
Arbiter for Financial Services

<u>Information Note related to the Arbiter's decision</u>

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(s) will be anonymised in terms of article 11(1)(f) of the Act.
