Before the Arbiter for Financial Services

Case ASF 117/2021

AY

(The Complainant)

vs

Papaya Ltd (C 55146)

(The Service Provider)

Sitting of the 14 November 2022

The Arbiter,

Having seen the Complaint[1] whereby in summary and in essence the Complainant states that he is disputing 24 charges totaling €7705.94 debited to his card account.

He further states that on 11 May 2021 these charges were made against his knowledge because to date he had no dealings with the company listed 'INF+AFR (Africatickets.com).' Furthermore, he insists that he received no correspondence via phone, email, or letter from this company informing him of any reason for the debits made. The company INF+AFR still to date does not exist.

The Service Provider first told him that it was a company named 'africatickets.com' and then 'guessed' it was a company called 'cresus casino'. The Complainant contacted this company and they stated that they have no record of him or the card being used. After refusing a chargeback, they told him

[1] P (Page) 2-3

that they will issue a Retrieval Request to the merchant which to date they have still failed to have any update on.

The Complainant further notes that Blackcatcard cannot supply him with:

- Proof of the transactions from the seller's end;
- The name of the seller other than INF+AFR (that does not exist);
- The address, email, or contact number of the seller;
- They refused to issue any kind of refund, even after having no idea who or why they paid his funds to a company that they cannot identify.

The Complainant further submits that although he is suffering from financial hardship as a result, they still ignored his refund requests.

Remedy Requested

The Complainant is asking the Arbiter to order the Service Provider to refund him the sum of €7705.94 together with interest at the rate of 30% of the total figure of €7705.94 per month from 11 May 2021. Thus, the total of €7552.05 by way of interest and the originally debited amount of €7705.94.

Having seen the reply[2] of the Service Provider where it states that:

Papaya Ltd (the Company) received the initial Customer complaint on 29 May although the letter was dated the 9th of May. The client disputed 24 (twenty-four) transactions amounting to EUR 7705.94 as authorized transactions. However, from the transaction total provided in the statement, the total amount is EUR 7274.84 for 25 transactions which is less than the amount disputed by the Customer.

Papaya Ltd started to investigate complaint that was related to unauthorized activity on 31 May 2021 as security-related complaints related to unauthorized charges are taken very seriously. The 'fair usage policy' is available to all customers at official company product website – https://blackcatcard.com/en/legal/papaya.fair-usage.html.

[2] P 46 *et seq*

We have replied to the Customer through our Support Chat and have also addressed his queries through e-mail when the Customer wrote to us in a timely manner clearly stating why the funds cannot be refunded. In regards to the Customer request which has been asked for on page 12 of the document as marked by the Arbiter, we consider that we have addressed the Customer's queries but we cannot divulge any information about our customers in general and especially if the said merchant is not a customer of Papaya Ltd.

In order to protect our Customers and in accordance with Directive No. 1 issued by the Central Bank of Malta, paragraph 72 (Authentication), the Company applies strong customer authentication where the payer:

a) accesses its payment account online;
b) initiates an electronic payment transaction;
c) carries out any action through a remote channel which may imply a risk of payment fraud or other abuses.

Therefore, the Company performed the following analysis:

- Identification if the strong customer authentication has been initiated and confirmed;
- Analysis of the payment description 'INF*AFR~~Lekki' that has been mentioned under the all reported charges and identification of the possible similarities made by the other Customers of the company that might have similar charges made by the 'INF*AFR~~Lekki'.
- Analysis of the past Customer activity and patterns;
- Analysis of Customer activity after the disputed transactions on the dates 7th-8th May 2021.

As a result of the internal investigation, Papaya Ltd has obtained the following result:

- **Identification if the strong customer authentication has been initiated and confirmed**.

  In accordance with the system log (refer to documents in appendices), all 25 online transactions to merchant INF*AFR ~~Lekki totaling €7274.84 in time period from 07-05-2021 till 08-05-2021 were authenticated by One Time Password (OTP), sent to Customer number +447368587075,

connected to Customer account on the basis of information provided by Customer during the onboarding process.

We would like to point out a discrepancy between the Customer claiming a refund of EUR 7705.94, while the total amount of these transactions is EUR 7274.84 as can be seen from Doc 'Card Transactional Report'. (The mentioned transactions were carried out in USD and the system converts this into EUR. The statement shows the value in EUR).

Papaya Ltd can also confirm that the same phone number and device that Customer used during the customer onboarding process for Blackcatcard is still being used up till now to carry out transactions. During the past two months, the Customer has carried out transactions in which an OTP by the Company is submitted to the same phone number and device, meaning that the Customer is initiating the payments and through the OTP, the Customer is confirming the payment.

Following Mastercard Chargeback rules acquirer/merchant can ignore a claim, referred to a transaction, confirmed by additional confirmation method, i.e., One Time Password, sent to a mobile phone. According to our logs, the disputed transactions were confirmed with an OTP which as described above was sent to the Customer's phone.

According to Blackcatcard Terms and Conditions paragraph (22) Cardholder takes full responsibility for keeping card sensitive data safe and failure to comply with this may be treated as gross negligence and may affect your ability to claim any losses.

- **Analysis of the payment description 'INF*AFR~~Lekki' that has been mentioned under the all reported charges and identification of the possible similarities made by the other Customers of the company that might have similar charges made by the 'INF*AFR~~Lekki'**

Papaya Ltd has performed transactions analysis by using its internal monitoring system and were able to identify a number of Customers who also performed transactions to INF*AFR~~Lekki. A sample of 4 clients were selected and requested to clarify such transactions. We have identified that this merchant may be used as part of the payment systems

for online gambling. We obtained replies from 2 of the clients and we have observed similar payment patterns which resulted in gambling activity.

- **Analysis of the past Customer activity and patterns**

  Papaya Ltd has performed analysis of the past Customer activity and identified that the MCC code 7995 (Gambling) corresponds to 52.36% of Customer activity followed by MCC code 7994 (Video Game Arcades/Establishments) with 8.73%. The following merchant descriptors have been identified: Bayton, betamo.com, bobcasino.com, Ilixium~~LuckyDays, MBETR0379, N1 Interactive Ltd and Skill On Net Limited.

However, by concluding the investigation results of case 'ASF 117/2021', the Company has a strong ground to say that all the reported 25 transactions totaling €7705.94 have been initiated and authorized by the Customer with use of OTP which as described above requires the user to input into the system the OTP code that is received on his phone which is linked to our system and which number was provided by the customer at onboarding stage. The authentication method shows that the input from the customer is required for the transaction to be executed.

Papaya Ltd requested refund for the transactions executed but this request was declined by Wordline (our third-party service provider, intermediary with MasterCard) since the transactions were carried out using OTP.

Unfortunately, our experience demonstrates that the customers who are using payment services for performing gambling-related activity (that is classified as a high risk) are more often to be prone to initiate chargebacks, disputes or reporting the possible fraudulent activity rather than ordinary customers who use our services for day-to-day card use. In this particular situation, the Company has refused to refund the amount debited to the Customer account and provide its decision to a Customer in a clear manner. We have observed that this is not the first time that the Customer has raised refund requests for similar activities.

Having heard the parties and seen the documents filed.

Considers

The Arbiter has to decide the case by reference to what, in his opinion, is fair, equitable, and reasonable in the particular circumstances and substantive merits of the case.[3]

The Complainant's position

In his final note of submissions, the Complainant made a series of allegations upon which he bases his request for the refund in connection with '24 transactions' that allegedly took place on his card account without his knowledge.

Basically, he states that he was defrauded and as such entitled to a refund by the Service Provider. In summary, he makes the following allegations:

1. That the bank's security system did not work. As a matter of fact, the Complainant states that he utilizes a bank service to have a secure environment for his money knowing that there is widespread cybercrime going around.

2. The Service Provider did not deem 24 transactions taking place over a period of 24 hours to be suspicious activity;

3. The Service Provider did not take reasonable action to confirm that the merchant was legitimate in accordance with MasterCard rules;

4. He was not fazed by the Service Provider's declaration that they followed the procedures of multi-factor authentication and that these multi-factor transactions were made through his cell phone. He contends that the Service Provider's proof in this regard is faulty and could be the result of cybercrime. He alleges that from the messages that took place during the period when the disputed transactions were made, he did not receive the OTP messages and, therefore, he could not have responded to authenticate the requests.

[3] Chapter (CAP) 555 of the Laws of Malta, Art. 19(3)(b)

5. That from his research, it transpires that the merchant is based in Nigeria while the IP address associated with the transactions is based in Finland '*which itself is questionable and should have raised an anomaly*'.[4]

6. That the Service Provider originally stated that the merchant was afritickets.com and when he highlighted that this company does not exist, they indicated that the company was africatickets.com. The former company was stated to be a gambling site whereas africatickets.com is a ticketing website.

7. The Complainant reiterates that the confusion in the name of the merchant runs counter to MasterCard rules because the name associated with these transactions on his bank statements is ''*INF*AFR Lekki 566*'' and the name *africatickets.com* does not show anywhere in his bank statements.

8. There appear to be two versions of the document provided by the Bank, one with the authentication list that shows consistently the name africatickets.com (a website that does not exist), and one with the transactions showing multiple different iterations of the website names, the majority of which are not valid websites.

9. The Complainant also suggests that he was the victim of a scam through the 'skimming' of his card.

10. Furthermore, the Complainant states that the volume of the transactions in question does not reflect his usual transaction activity. The 'bank' should have viewed this series of transactions as suspicious activity and should have put a hold on his card and contacted him to verify the transactions.

11. In summary, the Complainant reiterates that '*the bank failed in their obligation to safeguard my account from cyber-attack, failed in their obligations to pay due regard to my interests as their customer and to treat me fairly*'.[5]

[4] P. 72
[5] P. 73

The Service Provider

The Service Provider, Papaya Ltd, is a Financial Institution authorised and licensed by the MFSA under Schedules 1, 2, and 3 of the Financial Institutions Act. The Service Provider is thus authorised to provide card services and other ancillary services.

The Service Provider's Version

The Service Provider explained its position in its reply[6] and rebutted the Complainant's claims also in its note of final submissions.[7]

The Service Provider explains that:

1. The amount claimed by the Complainant is €7705.94 for 24 transactions. However, from the transaction total provided in the statement, the correct amount is €7274.84 for 24 transactions.

2. In accordance with para. 72 of Directive 1 issued by the Central Bank of Malta, the company applies strong customer authentication.

3. In this regard, the Company performed an analysis and obtained the following results:

    a) All 25 online transactions made to merchant INFR*AFR Lekki totaling €7274.84 were made by using the One Time Password (OTP) sent to the Complainant's mobile as indicated by him during the onboarding stage.

    b) That the same phone number and device that the customer used during the onboarding process for Blackcatcard is still being used by the Complainant to make transactions. He is still initiating payments through the OTP.

    c) According to their logs the disputed transactions were confirmed with an OTP which was sent to the customer's phone.

[6] P. 46 *et seq*
[7] P. 79 *et seq*

d) According to Blackcatcard (the card used by the Complainant) Terms and Conditions, para 22, the Cardholder takes full responsibility for keeping card sensitive data safe and failure to comply with this may be treated as gross negligence.

e) From its analysis, the Service Provider came to understand that INF*AFR Lekki is a merchant which may be used as part of the payment systems for online gambling.

f) From his past history, it results that the Complainant had about 61% of his activity related to gambling.

g) All 25 disputed transactions were initiated and authorised by the Complainant using OTP. This made it impossible for the Service Provider to succeed in a refund of the disputed transactions since OTP was used.

h) Experience has shown that clients using payment services for performing gambling-related activities are more often to be prone to initiate chargebacks.

i) The Service Provider observes that this is not the first time that the Customer has raised a refund request for similar activities.

Further Considerations and Conclusion

The Legal Framework

The Service Provider is a payments service institution and therefore the provisions of the Payments' Services Directive 2 (PSD2) applies. PSD2 came into effect on 13 January 2018 and was transposed into Maltese Law by virtue of Directive 1 (the Directive) issued by the Central Bank of Malta in accordance with Chapter 204 of the Laws of Malta.

According to the Directive, both the Service Provider and the user have certain specific obligations.

The user, in this case, the Complainant, is obliged *inter alia* to:

(a) *use the payment instrument in accordance with the terms governing the issue and use of the payment instrument, which must be objective, non-discriminatory and proportionate;*

(b) notify the payment service provider(s), or the entity specified by the latter, without undue delay on becoming aware of the loss, theft, misappropriation, or unauthorised use of the payment instrument.[8]

(2) For the purposes of Paragraph 45(1)(a), the payment service user shall, in particular, upon receipt of a payment instrument, take all reasonable steps to keep its personalized security credentials safe.

There is no contestation in the fact that the Complainant informed the Service Provider immediately after the 25 transactions in question were made. However, the whole question is whether the transactions were authorised by the Complainant or whether the transactions were the result of fraud by a third party.

The Directive also stipulates that:

49. (1) Without prejudice to Paragraph 47, in the case of an unauthorised payment transaction, the payer's payment service provider refunds the payer the amount of the unauthorised payment transaction immediately …'.

However, Article 50(1)(b) states that:

'The payer shall bear all of the losses relating to any unauthorised payment transactions if they were incurred by the payer acting fraudulently or failing to fulfil one or more of the obligations set out in Paragraph 45 with intent or gross negligence. In such cases, the maximum amount of EUR 50 shall not apply.'

This means that the Complainant will not be entitled to a refund if he acted with intent, gross negligence, or fraudulently.

However, it is to be noted that the Directive only sanctions a refund where in accordance with Article 49 the transaction was not authorised.

[8] Art. 45

So, the Arbiter has to establish whether the transactions were authorised by the Complainant or not.

Authorised transactions

The Complainant unequivocally states that he did not authorise the transactions:

'To this day I still don't know who took the money; I don't know where the merchant is; don't know the correct name of the merchant; I don't know what was purchased; I don't know how they took my card information, and how they managed to make these purchases and using a secure OTP or 3D Secure methodology which the bank says'.[9]

The Service Provider disputes the Complainant's assertion that he did not authorise the transactions and by way of proof makes the following observations:

That all the transactions in question were made by using the OTP sent by the Service Provider to the Complainant's mobile phone. The same mobile phone was used by the Complainant both prior to and subsequent to the disputed transactions.

From its analysis, the Service Provider came to understand that INF*AFR Lekki is a merchant who may be used as part of the payment systems for online gambling. From past history, it results that the Complainant had about 61% of his activity related to gambling.

All 25 disputed transactions were initiated and authorised by the Complainant using OTP. This made it impossible for the Service Provider to succeed in a refund of the disputed transactions. Experience has shown that clients using payment services for performing gambling-related activities are more often to be prone to initiate chargebacks.

The Service Provider observes that this is not the first time that the Customer has raised a refund request for similar activities.

[9] P. 61

The Complainant does not dispute these observations and the only reservation he showed was in regard to the identity of the merchant.

The Arbiter is convinced that once the 3D Secure was used with the Complainant's personal credentials and with the use of the OTP, there can be little or no doubt that the transactions were either made by the Complainant, or by someone authorised by him.

This case is very different from other cases decided by the Arbiter when the Complainant would have been tricked by a fraudster or where the Complainant would have been the victim of an organized scam. In this case, the Complainant himself used the security credentials supplied by the Service Provider and he himself made transactions similar to others he had made before.

Moreover, the Arbiter also considered the fact that the Complainant had made **similar requests** for a refund on other occasions. The Arbiter is morally convinced that the requests being made by the Complainant are not justified because he himself consciously authorised the transactions.

The Complainant alleges that he was a victim of fraud, but he did not produce any evidence to substantiate this allegation.

Decision

For the above-stated reasons, the Arbiter cannot uphold the complaint.

The costs of these proceedings are to be borne by the Complainant.

Dr. Reno Borg
Arbiter for Financial Services