Before the Arbiter for Financial Services

Case ASF 227/2024

AK

('Complainant')

Vs

Papaya Ltd.

Reg. C 55146

('Papaya' or 'Service Provider')

Sitting of 21 March 2025

Complaint[1]

Complainant states that his account with the Service Provider had been hacked and all the money stolen.

He states:

'*I received a message from the bank saying, "You have logged in from a new device, if you are not logged in please check immediately," with a link and when I used that link to log in to my account. I logged in to the fake website and that is how my money was stolen. That link was exact copy from the bank app. Then I received an email from the bank warning about phishing with a link*

(https://blackcatcard.com/blog/how-to-protect-your-payment-data-on-the-internet) to an article about How to protect your payment data on the Internet? And at the end telling me that my money is safe.'[2]

He complains that four unauthorised transfers were made from his account on March 30, 2024, to another account at Papaya held by a person whom he did

[1] Pages (p.) 1 - 6 with attachments p. 7 - 25
[2] P. 2

not know for a total of €3566. These were affected in the space of 2 minutes between 22:53 and 22:54.[3]

He questions how the hacker got his phone number and how his confidential information had been stolen. He complains that the Service Provider only sent him warnings to be careful of *'phishing after four months from the hacking'.*[4] He further stated that the hacker was still sending him messages.[5]

By way of compensation, he originally claimed refunds of the stolen funds and a penalty for the identity theft and emotional distress for a total of €100,000. At the hearing and subsequent submission, the compensation sought was raised to €250,000.[6]

Reply of Service Provider

In their reply of 20 December 2024, the Service Provider stated:

'We would like to present the following response to clarify our position and provide relevant context for the case:

1. ***Overview of the Transactions:***

   On March 30, 2024, a series of transactions totalling 3,566 were made from [the Complainant's] account to a third party, Ms xxx. [The Complainant] has claimed that these transactions were unauthorised and believes Papaya Ltd. is responsible for ensuring the security of his account and card.

2. ***Security Measures and Terms of Use:***

   At Papaya Ltd., we employ robust security measures to protect our clients' accounts and cards. However, as per our Terms and Conditions, clients are required to:

   - *Keep their card details, login credentials, and authentication information secure and not disclose them to third parties.*

[3] P. 7; 13
[4] P. 3
[5] P. 25
[6] This being the maximum compensation that the Arbiter can award in terms of Article 21(3)(a) of CAP. 555 of the Laws of Malta

- *Notify us immediately if they suspect any unauthorised access or loss of control over their account information.*

The client's acknowledgement of these terms forms the foundation of our mutual responsibilities.

3. ***Investigation of the Incident**:*

   Upon reviewing the transactions and consulting our internal systems, we have confirmed the following:

   - *All transactions were properly authenticated using the client's credentials.*
   - *We did not detect any breach of our systems or evidence of unauthorised access originating from Papaya Ltd.'s infrastructure.*
   - *The transactions appear to have been initiated using information under the sole control of the account holder.*

4. ***Position on Responsibility:***

   While we deeply sympathise with the inconvenience caused to [the Complainant], it is our position that Papaya Ltd cannot bear responsibility for unauthorised transactions resulting from the compromise of the client's personal account details. As stated in our Terms and Conditions, clients bear full responsibility for the safekeeping of their credentials and assume liability for any losses arising from the compromise.

5. ***Proposed Resolution and Assistance**:*

   We remain open to collaborating with the Financial Arbiter to address any questions or concerns related to this matter.'[7]

Hearing

At the hearing of 11 March 2025, the Complainant largely repeated the claims in a note titled:

[7] P. 31 - 32

'Request for Compensation Due to Financial Loss and Security Negligence – Papaya Ltd'.

This note is now being admitted in the proceedings together with a copy of 3 SMS messages received from BlackCat in December 2023.[8]

Papaya maintained that they had issued proper warnings to client even before December 2023 not to disclose the secret access credentials to third parties whilst Complainant maintained these were only received after the event causing the loss.

Asked why he initially reported only 3 fraudulent transfers and then, after 6 months, he filed a complaint including a 4th transaction, he said it was a mistake.

In their evidence, Papaya stated:

'***Actually, I have the chat with the client where he contacted the Support Department of Papaya, Blackcatcard, where he reported three transactions on 31 March 2023.***

We have confirmation from our Support team that the only way the client could log in and authorise these transactions was by providing the PIN code; and if the client did not provide this PIN code and his log in credentials to third parties, then it actually could not work.

So, we understand that the client had actually provided this PIN code and the password on the link that he had received from the Spanish number despite knowing that we are a Maltese company.

On 1 April we had asked him whether he had reported this issue to the police and he informed us that the last time that he had used the account is the day when the suspicious transactions had appeared and after that he did not go to the police.

After 1 April, when we had communicated with the client, the account was blocked for one week because we wanted to make our own investigation and then, we had informed the client on 8 April that it was actually the responsibility of the client when he presented his credentials to the third party because actually he had done this and we have the evidence that he had done that.

[8] P. 39 – P. 42

Then, the client disappeared until 30 October where he asked us to provide him with his authorisation again via email.

The account was not blocked but the client did not have access from his side and contacted us on 30 October by email.

On 4 November, he asked us how much money had been stolen from his account. So, actually, he confirmed that he did not provide access to his account to anyone.

On 12 November, eight months after the incident, he contacted our AML Department to investigate the situation. We informed him that we had started the investigation. And on 12 November he informed us that there were not only three transactions but there was also the fourth transaction of €60. All of these transactions had been done in one day.

So, after he filed the complaint with the Office of the Arbiter, we have investigated and found out that the client had provided his credentials, the login and the password to the third party and, on the same day, the money had been transferred to another account. We have no steps how to investigate where this money went after the client had provided his credentials to the third party.'[9]

The Complainant made no cross-examination of Papaya's evidence but, upon being questioned by the Arbiter, he stated he did not know the beneficiary of the Papaya account where his funds were transferred.

Service Provider said the funds were transferred immediately from the recipient account to an account outside the bank and they had no opportunity to block the funds when Complainant reported the loss the day after the event.

Analysis and consideration

The Arbiter harbours doubts about the genuine qualities of this Complaint.

These doubts are sourced by the following:

1. Complainant presented text messages[10] ostensibly received on the SMS channel of communication with Papaya which are dated between 11 and 18 December 2023, claiming that the last message was sent by the hacker who penetrated the channel. The theft was executed on 30 March 2024

[9] P. 35 - 38
[10] P. 42

and there is no evidence that the messages of December 2023 had anything to do with the claimed fraud payments.

2. Complainant states that hacker is still sending him 'annoying messages'.[11] It is not understood why hacker would use a Spanish number for this message rather than continue using the channel of Papaya which Complainant claims was penetrated by the hacker.

3. Complainant filed his complaint with Papaya on 07 November 2024,[12] more than 7 months after the alleged scam.

4. It is quite untypical for a scammer to transfer the funds to an account with the same institution holding the account from where the funds were stolen. This raises doubts on whether the holders of both accounts were in fact in tacit co-operation.

5. Genuine victims of scams normally would be happy to recover their lost funds. In this case, the Complainant is seeking exorbitant compensation for claimed emotional distress for 70 times the amount reported stolen.

Decision

The Arbiter considers this Complaint as frivolous or vexatious and, in terms of Article 21(2)(c) of CAP. 555 of the Laws of Malta, is declining to exercise his powers under this ACT CAP. 555 and is hereby closing this file.

Each party is to bear its own costs.

Alfred Mifsud
Arbiter for Financial Services

[11] P. 25
[12] P. 7

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.