Before the Arbiter for Financial Services

Case ASF 330/2025

IN

('Complainant')

vs

MiFinity Malta Limited

Reg. No. C 64824)

('MML' or 'Service Provider')

Sitting of 15 July 2026

The Arbiter,

The Complaint[1]

Having seen the Complaint filed on 12 December 2025 where Complainant holds that several transactions amounting to €12,000 were made on 27 October 2025 from her wallet account with MMF without her authority.

She argues that these payments were allowed to go through without being properly authorised by Strong Customer Authentication (SCA) in terms of Article 97 of PSD 2[2] and that MMF enjoyed none of the exemptions from applying such SCA in terms of Articles 11 – 18 of delegated regulation EU 2018/389.

[1] Pages 1 - 8 with attachments 9 - 30

[2] Article 97 of EU Directive 2015/2366 (PSD2) obliges Payment Service Providers (PSPs) to apply strong SCA where the PSU (Payment Services User) makes on-line payments remotely.

She contends that these payments and a password change were carried out with unauthorised access to her account and accordingly she holds MMF responsible for her loss and requests compensation of the full €12,000 loss she claims to have suffered.

Reply of Service Provider

In their reply[3] of 18 January 2026, MMF submitted that Complainant had an account with MMF since 11 March 2025 and used her account for gaming activities, i.e., depositing and receiving funds from gaming operators. No transaction prior to 27 October 2025 was disputed.

They maintain that their e-wallet uses strong SCA ensuring that only the account holder has access to and can make transactions on her account. The SCA was applied every time she logged into her account and for each payment effected and MMF was not relying on any exemptions for not applying SCA. They maintain:

"Following the transactions, a password change was requested on the account at 19:08 in the course of an authorized session, followed by 5 successful logins from the same IP addresses, which were used for previous undisputed password changes, transactions and withdrawal requests.

As the Customer insisted on unauthorized access in the correspondence with the Company, she was informed that if such transactions were not authorized by her, they were most likely initiated by a third party using her devices. However, the Customer has never confirmed that any third party has accessed her account.

Although the Company has no record of any compromise of its platform and fraud was not detected by the monitoring systems, due to the claims of unauthorized access by the Customer, the Company disabled her account.

Based on the above facts the refund was denied by the Company."[4]

……

"*Although the patterns of the transactions carried out on 27/10/2025 might indicate a so-called 'Chasing Losses', the Company cannot investigate merchant-*

[3] P. 35 - 40 and attachments p. 41 - 87
[4] P. 36

specific gambling losses or deposits since the Company is not a gaming operator and that any disputes regarding gambling outcomes must be directed to the gaming operator as it is their sole responsibility and not of the Company.

Furthermore, the Company as a financial institution is not responsible for affordability checks and responsible-gaming compliance.

Essentially, the Company confirms that it fully adheres to and has applied its regulatory obligations properly and without delay.

Moreover, the Company would like to emphasise that it cannot assume liability refunding Mrs. IN's transactions for the following reasons:

1. *The account was opened by the Customer.*
2. *The account was verified in line with the AML policy and AML/CFT obligations of the Company.*
3. *The claim is inconsistent and has changed from 11,000 Euro to 12,000 Euro without any further explanation by the Customer.*
4. *Prior to 27/10/2025 no transaction was disputed.*
5. *The Customer has not specified which transactions she claims unauthorized from all 25 transactions carried out on 27/10/2025.*
6. *All the transactions were considered internal transactions as no funds left the Company, therefore no further notification was required to the Customer`s registered device.*
7. *Transfers to the gaming operator can only be initiated from the Customer`s account at the gaming operator.*
8. *All transactions on the Company`s Platform were initiated following authorization sessions, which were successfully completed.*
9. *The Customer has not confirmed any unauthorized third-party access to her devices.*
10. *The Customer`s IP addresses used during the relevant transactions, password change and the logins following the passport change were matching with the previously identified IP addresses.*

11. *The Customer has never confirmed if such funds were lost, i.e. not credited to her account at the gaming operator.*

12. *The Customer has not reported any unauthorized access to her account with the gaming operator.*

13. *The Company has no access to, or visibility of, the customer's gambling account and activity.*

14. *The Company does not financially benefit from gambling outcomes.*

15. *Refunds for voluntary payments are legally and operationally impossible.*

For these reasons, the Company is not responsible and/or liable to refund the claimed sum of EUR 12,000 consisting of funds of claimed unauthorized internal transactions."[5]

Hearing of 12 May 2026

During the hearing,[6] Complainant reaffirmed that the payments were not authorised by her. She confirmed that she used her account to gamble with online operators and that in the past she won and lost but not huge amounts.

"Asked how I used to make these transfers, I say to pay in there are the deposit merchants like Skrill or, for example, MiFinity. I log into MiFinity account, and then I was able to send the money.

Asked how I used to send the money, I say by using email address, password, and the authentication code, which I usually get on my phone for each and every transaction."[7]

When asked if she had checked with the counterparty of the disputed transactions, whether funds were received on her account with them, she stated that no information was given to her about who was the counterparty to see if she had an account with them.

The Arbiter ordered MMF to explain who the beneficiary of these transfers was, as once they had confirmed that payments were not sent out of the MMF

[5] P. 38 - 39
[6] P. 88 - 93
[7] P. 90

system, they should have a clear view of who the counterparty was. They should provide such information to Complainant to enable her to take up the matter with the identified counterparty.

The Arbiter ordered MMF to explain whether the actual payments were made with SCA for every transaction (as they maintained during the hearing) or whether MMF relied on regulatory exemptions as indicated in their Reply.

Submissions following the first hearing

By letter and email of 18 May 2026,[8] MMF indicated the counterparty was BlueOceanGaming operating under tradename HazCasino.

They also submitted extensive attachments which the Arbiter summarises as follows as being the most relevant:

1. Extract of the disputed payment effected on 27 October 2025 between the hours of 12:55 and 17:02[9]

2. Annexe 2 showing the extensive logins to Complainant's account on 27 October which continued on the next day showing a distinct picture from the login pattern in prior days.[10]

3. Annexe 3 – Proof of 2FA; this was accompanied by a video showing the SCA being the mobile APP and facial recognition[11].

4. Gameplay extracted from the counterparty account showing extensive transactions on the day on an account linked to Complainant's e-mail address[12].

By reply on same date,[13] Complainant provided evidence she held no account with HazCasino and that the Gameplay provided contradicts earlier submissions of MMF that they have no access to data stored by the gaming operator. She repeated her claim that the gameplay is no evidence that the transactions were authorised by her.

---

[8] P. 95 - 98
[9] P. 99
[10] P. 100 - 102
[11] P. 103
[12] P. 104 - 106
[13] P. 108 -110

By a decree issued on 29 May 2026,[14] the Arbiter demanded clarity on the conflicting claims about Complainant having an account with HazCasino who was identified as the counterparty for the disputed transactions.

On 01 June 2026,[15] evidence was submitted that the counterparty was Stakeprix Casino not HazCasino which were both brands operated by the Versus Odds B.V. as licence holder. They confirmed that their records show that email belonging to Complainant is linked to an account she holds with Stakeprix Casino.

At the hearing of 18 June 2026,[16] Complainant denied she held an account with Stakeprix Casino.

No further submissions were made and both parties agreed that the case is put for decision based on evidence provided.

Decision

Having considered all the evidence and in line with the obligation to decide by reference to what, in his opinion, is fair, equitable and reasonable taking into consideration the particular circumstances and substantive merits of the case[17], **the Arbiter does not uphold this complaint** for the following reasons:

a. Sufficient evidence has been provided that these payments were transferred to an account with a casino operator with whom her e-mail was registered on the relevant account (even though she denies having such an account).

b. Sufficient evidence has been provided that these transfers were affected with proper SCA procedures meaning that they were either authorised directly by the Complainant or by someone who had access to her device and her credentials (which is improbable given that facial recognition was used as one criterion for the SCA).

[14] P. 110 - 111
[15] P. 112 – 113
[16] P. 114 - 116
[17] Article 19 (3)(b) of CAP. 555 of the Laws of Malta.

c. No evidence was provided that there was any compromise on the security of MMF platform nor that the counterparty platform was compromised (although this would not have necessarily thrown any responsibility on MMF).

d. Although the transaction and log-in pattern on 27 October 2025 was atypical to prior history, it is not uncommon for gambling clients to fall into 'chasing losses' condition which causes such activity spikes. MMF, as a PSP, is not responsible for affordability checks and responsible gambling obligations applicable to licensed casino operators.

The Complaint is accordingly hereby dismissed, and each party is to bear its own costs of these 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. Personal details of the Complainant(s) will be anonymised in terms of article 11(1)(f) of the Act.