DRN-6205953

The complaint

Mr A complains that Modulr FS Limited, trading as HyperJar Limited, won't refund an unauthorised transaction carried out from his account.

What happened

Mr A has an account with HyperJar.

Mr A saw an advert on a social media site for a chocolate bundle priced at £2.59. Mr A clicked on the advert and on being sent to another website he entered his card details in an attempt to purchase the items.

Mr A then received a One Time Passcode (OTP) from HyperJar which he entered into a link he received, from what he thought was a company I'll call G, in the belief he was authorising the purchase.

The next day Mr A visited the website again in an attempt to purchase another 'chocolate bundle', he received another OTP which he again entered into a link sent to him.

A few days later Mr A noticed a transaction for £80.10 on his HyperJar card to a supermarket which he didn't authorise. He raised a claim with HyperJar, but they didn't uphold it – concluding that the payment was carried out with a digital token set up via an application I'll call GPay. This was set up using Mr A's card details and an OTP sent to his phone number. Therefore, they thought the payment was authorised.

Mr A wasn't satisfied with HyperJar's response so complained to our service.

One of our Investigators looked into Mr A's complaint. They thought HyperJar hadn't shown sufficient evidence to demonstrate how the token was set up so it wasn't fair for them to conclude it was authorised. And HyperJar should refund the disputed transaction of £80.10 plus 8% interest from the date of the transaction to the date of repayment.

Mr A agreed, but HyperJar didn't. They argued that they'd shared sufficient evidence of when the token was created. And they thought Mr A acted with gross negligence in sharing the OTP codes.

As Mr A didn't agree the case was passed to me to decide.

On reviewing Mr A's case I reached a different conclusion to our Investigator. I agreed that Mr A didn't authorise the disputed transaction, however I thought in sharing the OTP sent to his device Mr A acted with gross negligence. And therefore, it was fair for HyperJar to find him liable for the payment.

Mr A didn't agree, in summary he said:

- Gross negligence is a high bar. He was acting as a reasonable consumer responding to a professional looking advertisement on a mainstream social media platform. And believing a promotional offer is a common human error.

- There's a difference between being careless with a device set up and being grossly negligent – he never saw nor was he warned about an £80 charge.

- Criminals use cognitive load and urgency to bypass a person's normal defences. When he entered the code he thought he was on a legitimate payment portal, and the Financial Conduct Authorities (FCA's) guidance recognises that even clear warnings can be ignored during the 'heat' of a sophisticated scam.

- HyperJar have failed to meet the burden of proof required to establish exactly how the fraud was executed.

As Mr A didn't agree I've proceeded to reconsider my findings below.

What I've decided – and why

I've considered all the available evidence and arguments to decide what's fair and reasonable in the circumstances of this complaint.

I've firstly considered whether Mr A authorised the disputed transaction. HyperJar have been able to share some details regarding how the payment was authenticated, including that two tokens were set up via a digital wallet, but I haven't seen specific evidence to show this token was used to make the disputed transaction. However, despite this I think it's the most plausible explanation for how the payment was carried out.

I've moved on to consider whether Mr A authorised it, and I'm satisfied that he didn't. I say this as I accept Mr A's version of events for how the payment was carried out, without his consent, as the most likely explanation.

Usually when a payment is unauthorised the business is liable for the payment, however HyperJar have argued that Mr A acted with gross negligence. So I've moved on to consider this.

I'm afraid having done so I think Mr A did. The FCA says:

'…we interpret gross negligence to be a higher than the standard negligence under common law. The customer needs to have shown a very significant degree of carelessness.'

I've seen a copy of the messages sent to Mr A which contain the OTP. Mr A agrees he received these and entered them into a link he believed was from G. The messages said:

'… is your HyperJar card OTP for GPay. Do not share it with anyone. Your HyperJar card ending in … has been added to GPay'.

I'm satisfied that the messages sent to Mr A were clear in stating he shouldn't share the OTP with anyone. And they also advised that his card had now been added to GPay.

Mr A has argued that he was responding to a professional looking website on a well-known social media platform. And even clear warnings can be ignored during the heat of a sophisticated scam. Unfortunately, Mr A's been unable to share any evidence of the advert or website where he made the purchase. From what Mr A's described about the scam and the lack of evidence he's been unable to share it's not possible for me to conclude that the advert and website appeared professional or this was a sophisticated scam.

I've thought about whether Mr A's sharing of the code showed a very significant degree of carelessness and I'm afraid I think it did - I think firstly the messages are clear in advising the

OTP shouldn't be shared. Secondly Mr A was under the belief that he was sharing the OTP to make a purchase for £2.59 – however the messages show no indication of this, instead they state Mr A's card has been successfully added to GPay.

For the reasons I've outlined above I think Mr A acted with gross negligence, and it follows I won't be holding HyperJar liable for the payment.

My final decision

My final decision is I don't uphold his complaint.

Under the rules of the Financial Ombudsman Service, I'm required to ask Mr A to accept or reject my decision before 18 May 2026.

Jeff Burch
Ombudsman