DRN-6055779

The complaint

Mr T complains that Think Money Limited has unfairly declined to reimburse a payment he didn't authorise.

What happened

In February 2024, Mr T received a call from a scammer impersonating Think Money. He recalls logging into his app to decline a payment and being asked to enter an OTP into his keypad. Mr T says when he received a message about a new device accessing his account he replied "Block". He's disputing a payment for £888 to a new payee made using the newly set up device.

Think Money declined to reimburse Mr T – it held him liable based on the secure information it thought Mr T likely shared and the warnings it had provided to him at the time.

When Mr T referred his complaint to our service, the investigator upheld it. In summary they concluded the payment was unauthorised and that Mr T hadn't failed in his obligations to keep his secure information safe with gross negligence.

Think Money didn't agree – it said:

- The user of the new device would have needed the following to access the banking app: the four-digit OTP it sent to Mr T by SMS, Mr T's six-digit passcode, information about Mr T and his account.
- It gave Mr T a relevant warning when he logged into his banking app that day, including before he shared the OTP which said.
- Mr T logged into his banking app on his device several times after it sent him a message about a new device being set up, before and after the payment was made.
- Mr T didn't send a "Block" message to the number provided in its SMS until after the payment had been made.

The investigator explained why this didn't change their findings in the circumstances. As Think Money didn't agree, the matter was passed to me for consideration by an ombudsman. I issued my provisional decision on 15 December 2025 explaining why I didn't intend on upholding the complaint.

Mr T didn't accept my provisional decision and reiterated that his passcode had been his date of birth.

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.

Having done so, I'm not upholding this complaint – I'll explain why.

Has Think Money acted fairly in holding Mr T liable for the payments?

It's common ground that Mr T was the victim of a scam, and that the disputed payment was made by the scammer using a newly set up device. I've considered how this was done.

Think Money has explained that to log into Mr T's banking app on a new device, the following was needed:

- The customer's account number, date of birth and email address.
- A four-digit OTP which is sent to the registered mobile number.
- The customer's personal six-digit passcode.

Think Money has also provided evidence that the OTP and passcode were entered correctly from the new device at the time of the scam - before the passcode was changed and the disputed payment was made.

Mr T recalls being asked some security questions at the beginning of the call with the scammer. He says he was told about fraudulent payments including a £15 payment which he then went into his banking app to decline. The scammer then said they would check the account – they called back reassuring Mr T everything was fine and said that he'd be sent a four-digit pass code to help him change the security code on his account. Mr T says the scammer seemed legitimate, so he went ahead and input the four-digit code using his keypad, and that he didn't share this verbally as he knew not to. Mr T has consistently said he didn't share his passcode, but when asked by our service Mr T has speculated that it could have been guessed because it was the first six-digits of his date of birth.

Think Money says this isn't possible as its system doesn't allow the passcode to include the customer's date of birth due to this being easily guessable.

I've also listened to calls between Mr T and Think Money – when he reported the scam and discussed his claim. Here Mr T says that he was asked for the OTP and provided it. He described that the scammer said *"you're gonna have to tell me what that number is".*

Where evidence is incomplete, missing or contradictory, I need to determine what I think is more likely than not to have happened. I do this by weighing up what I do have and making a finding on the balance of probabilities.

Having done so, based on the above I think it's more likely than not that Mr T shared both the OTP and his passcode with the scammer over the phone.

I also note that the evidence from Think Money shows that Mr T logged into his banking app from his device five times during the scam before the disputed payment was made. Once before he received the OTP, and four times after the passcode was changed (using biometrics). It isn't clear why he did this.

I can understand why someone panicking about their account being under attack might not read a message properly, but Mr T has described being reassured the account was safe. So, it's not clear why he didn't send a "block" message to the number provided in the SMS messages from Think Money until after the payment was made – around an hour after the SMS was sent to him (and instead replied block which showed as undeliverable).

Think Money has also said every time Mr T logged into his banking app he would have been shown this warning message *"We will NEVER ask you to share a 4-digit code from a text, over the phone, or by typing it into your telephone keypad. Sharing your 4-digit code is how scammers access your banking app. If you're asked to share this code, end the call, text 'BLOCK' to 81122 & call 01617795000."* Mr T says he doesn't recall reading this.

Under the PSRs – the starting point is that Mr T is liable for authorised payments. I consider that it would also be fair for Think Money to hold Mr T liable if he had delegated the ability to make payments on his behalf, even if the scammer went beyond the scope of what they had agreed to.

In the event that the payments were unauthorised, Think Money could also fairly hold Mr T liable for the payments if he had failed in his obligation to take all reasonable steps to keep safe personalised security credentials relating to a payment instrument with intent or gross negligence.

As the call came from a *"no caller ID"*, I think it would have been reasonable for Mr T to have been on guard about the origin of the call. While the scammer was able to mimic a suspicious payment, I think Mr T still should have been concerned when asked to share a secure code and his passcode. Particularly as the purpose of a passcode and the risks attached to sharing it are well-known.

Without an explanation from Mr T, particularly around why he shared his passcode (that I have concluded above he did share) – there's no way to know what he agreed to. Similarly, without knowing how the scammer persuaded Mr T to share this, what risks he appreciated, and what reassured him, I don't think it would be reasonable to conclude that Mr T didn't fail with gross negligence to keep his secure information safe. Mr T has had the opportunity to clarify this.

It follows that, based on the information available, I don't consider that Think Money has acted unfairly in holding Mr T liable for the payments.

Did Think Money miss an opportunity to prevent Mr T' loss?

An Electronic Money Institution ("EMI") such as Think Money is expected to process payments and withdrawals, in accordance with the PSRs and the terms and conditions of the customer's account.

But, taking into account longstanding regulatory expectations and requirements, and what I consider to be good industry practice, Think Money ought to have been on the look-out for the possibility of fraud and made additional checks before processing payments in some circumstances.

Having considered when the disputed payment was made, it's value and who it was made to, I'm not persuaded Think Money ought to have found it suspicious, such that it ought to have made further enquiries than it did of Mr T before processing it.

I've thought about the fact that it was a new device making the payment, but Think Money took steps to check whether the person using it was authorised. Including requiring an OTP sent to Mr T and his passcode to log in. It also sent Mr T an SMS message flagging that a new device had been used to access his account which asked him to take steps if this wasn't him. So, I don't think this would be enough to expect a further intervention without the payment itself presenting as higher risk.

I've considered Mr T's point that there were multiple passcode resets before the payment was made. While a passcode change can be a relevant factor in identifying risk to an account, here the person changing the passcode had already used the existing passcode to access the account. So, I don't think it would be proportionate to expect a further intervention given the relatively modest payment amount and two-factor authentication steps that had already taken place.

For these reasons, I don't consider that Think Money needed to do more to intervene in the circumstances.

Should Think Money have done more to recover Mr T's funds?

The disputed payment was a faster payment - Think Money contacted the receiving bank to request the funds be returned and it was informed that the funds were already withdrawn from the account. As the funds were utilised within around ten minutes of the payment being made, I don't consider that Think Money could have done anything more that would have resulted in Mr T receiving the funds back from the receiving bank in the circumstances.

My final decision

My final decision is that I don't uphold this complaint.

Under the rules of the Financial Ombudsman Service, I'm required to ask Mr T to accept or reject my decision before 3 February 2026.

Stephanie Mitchell
Ombudsman