DRN-5669604

The complaint

Mr B is complaining that Think Money Limited hasn't agreed to refund payments he says he didn't make.

What happened

On 16 February 2024 Mr B received two calls from someone (who I'll call the scammer) who said they were from Think Money. Over the course of the two calls, they told Mr B his account had been compromised, and someone had tried to use his card to make payments, but they would sort this out for him. The scammer was able to give him details of transactions and direct debits and asked him to confirm that he recognised the payments. They asked him for his 6-digit passcode so they could access his account and cancel the transactions.

Mr B says he gave his date of birth and address to the caller and he also shared his passcode to access Think Money's app. Mr B received a text message with a one-time passcode (OTP) which he apparently then shared with the caller, which allowed another device to be registered to Mr B's account. He then received another text message which explained that a new device had been used to access his account and if this wasn't him, he should reply with BLOCK or call Think Money. Mr B didn't reply to this message at that time and says the caller told him to ignore it and he'd get some more similar messages.

Two faster payments were then made from Mr B's account to a new payee. The first payment made was for £990 and the second payment was for £490.

There was an attempt to register another device to Mr B's account just before 9.00pm. However, this time Mr B, after discussing what was happening with someone else, replied to Think Money's text to say it should be blocked, and at this point the scammer hung up on him.

Mr B tried to call Think Money at around 9:30pm but by that time, its office was closed for the weekend. He tried to call again the following day, but he couldn't speak to anyone until 19 February 2024 when he reported the scam.

Think Money attempted to recall the payments, but it was told the funds from both payments had left the recipient's account shortly after they were received. It told Mr B it wouldn't be able to return the funds to him.

Mr B complained to Think Money about what had happened. Think Money replied to his complaint to say, in summary, that it hadn't found it was liable to refund the disputed payments.

Mr B referred his complaint to the Financial Ombudsman Service. Our Investigator thought Mr B's complaint should be upheld and that Think Money should refund the disputed payments to him, with 8% simple interest. Our Investigator said, in summary, that Mr B hadn't authorised the payments and neither had he failed with gross negligence or intent to keep his secure details safe.

Think Money says, in summary, that Mr B acted with complete carelessness in taking the actions he did in sharing personal information and security details, and ignoring warnings he received. So, it maintains that it shouldn't be liable to refund the payments.

Mr B's complaint has now been passed to me for review and a decision.

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 B authorised these payments. This is relevant as, in line with the Payment Services Regulations 2017 (PSRs), he would generally be liable for payments he authorised – whereas Think Money would be liable for unauthorised payments.

The PSRs specify that authorisation depends on whether the payment transactions were authenticated correctly – and whether Mr B consented to them. It's not disputed the payments were authenticated correctly (as in, the correct payment steps were completed). So, I've gone on to consider whether Mr B consented to them.

The PSRs specify how consent is given – it must be in the form, and in accordance with the procedure, agreed between Mr B and Think Money. I've reviewed the terms and conditions of Mr B's account with Think Money at the time the payments were made. These set out how transactions are authorised, as follows:

"Any transaction on your account (other than from your Think Money card) will be treated as authorised by you if you:

a) tell us you have authorised it in writing (by letter, a signed payment slip, a text message, an email or through our mobile app using your secure login details or security information, either provided at the time of the transaction or stored on your device);

b) authorise the transaction by phone (calls may be recorded); or

c) authorise a third-party provider to access your account to make payments (see the Third-party providers section)."

I appreciate that there are some discrepancies here in relation to what information Mr B recalls sharing and when, over the course of the two calls he received. However, it doesn't appear to be in dispute that it was the scammer and not Mr B that gave the payment instructions here, after Mr B shared details which allowed them to access his Think Money account through the app. It follows Mr B hasn't used the agreed form and procedure himself to consent to these payments.

While it does seem that Mr B shared personal and security details which enabled the scammer to access his Think Money account and make payments from it, he did so on the understanding he was protecting his account. So, I don't think he understood he was, in fact, allowing someone to access his account with the intention of making payments from it.

Considering that Mr B was tricked into allowing someone to access his Think Money account, I don't think it would be fair to say he gave a third-party permission to consent to payments on his behalf. It follows that I'm satisfied the disputed payments were unauthorised. This means the starting position under the PSRs is that Think Money is liable to refund them.

Did Mr B fail to keep his security details safe with gross negligence or intent?

Think Money submits that even if these payments are to be considered as unauthorised, it shouldn't be held for liable them. That's because it thinks Mr B failed with gross negligence to keep his personal and security details safe – something which, if proven, would mean he wouldn't be entitled to a refund under the PSRs.

Think Money's terms and conditions also refer to this, as follows:

"You are responsible for all losses due to an unauthorised transaction if you have acted fraudulently or you have failed to do any of the following (whether this was intentional or due to gross negligence).

a) Tell us as soon as possible about the loss, theft, or unauthorised use of your Think Money card or account login details.

b) Take all reasonable steps to keep your security details safe.

c) Keep to these Ts and Cs."

I've reflected on the circumstances that led to the scammer gaining access to Mr B's security details, including his app passcode and the OTP to register a new device. The text message including the OTP did include a warning not to share the code with either Think Money or the police. He also didn't act on the first text message he received which said that a new device had accessed his account.

But Mr B says he was reassured by the scammer who said the text messages had come from them. They also read out the text of one of the messages to Mr B as he was reading it and said he would receive more of these messages, which would likely have further reassured Mr B because the caller was apparently familiar with the text of the messages. I'm also taking into account that at the time Mr B shared the information he would have been being put under a lot of pressure to act quickly to protect his account. And from what he's said, and also from what we know about how these types of scams generally operate, he was experiencing techniques from the scammer designed to distract him from having time to think more carefully about what he was doing.

Think Money has also told us that it regularly shows scam warnings to its customers when they access the app, and Mr B had been shown relevant scam warnings before he experienced this scam. This included a scam warning that was shown to him when he logged into his app the day before the scam took place, warning him never to share an OTP. So, it thinks Mr B ought to have been aware of this type of scam before he fell victim to it. But I don't think these warnings would necessarily have resonated with Mr B to the extent that he ought to have realised the caller was a scammer, given that he wasn't experiencing the scam at that time the warnings were shown to him.

I appreciate that Think Money says that it was still open until 6pm when the payments took place just after 5pm – so it thinks Mr B could have reported the scam sooner. But it's clear that Mr B didn't realise he'd fallen victim to a scam until he received the second call, which was around 9pm. But by this time, the funds had already been moved on from the receiving account. And I can see he first attempted to call Think Money at around 9.30pm, shortly after realising he'd been scammed.

This isn't to say Mr B acted perfectly reasonably here. Under the impression he was protecting his account, he did take a number of steps in sharing different pieces of information which led to a third-party gaining access to his account and making payments

from it. But to conclude that Mr B failed with gross negligence I'd need to conclude that he acted with a very significant degree of carelessness. And having considered the circumstances carefully, I'm unable to reasonably conclude that Mr B's loss was caused by him failing with gross negligence. I'm also not persuaded that Mr B intentionally failed to keep his security information safe, because he was satisfied he was speaking with Think Money.

In this case, I have found that the payments were not authorised and that Mr B hasn't failed with gross negligence or intent. It follows that, in line with the PSRs, I don't consider Mr B can be fairly held liable for these unauthorised payments and Think Money must put things right – by refunding his losses from the payments alongside 8% simple interest per year to compensate him for the time he's been out of pocket.

My final decision

For the reasons I've explained, my final decision is that I uphold Mr B's complaint.

Think Money Limited must:

- Pay Mr B the total of the unauthorised payments - £1,480; and
- Pay 8% simple interest per year on this amount, from the date of the unauthorised payments to the date of settlement (less any tax lawfully deductible).

Under the rules of the Financial Ombudsman Service, I'm required to ask Mr B to accept or reject my decision before 13 February 2026.

Helen Sutcliffe
Ombudsman