DRN-5157390

The complaint

Miss D complains that Think Money Limited won't refund payments she didn't make or otherwise authorise.

What happened

On 20 February 2024, Miss D received a call from someone purporting to be from Think Money's fraud department. They said they suspected fraudulent activity on her account. Miss D says they already had her account details and read out recent transaction activity on her account and asked her to confirm if she recognised them. Miss D states she recognised some but not all, and the caller then proceeded to discuss her accounts held with other firms.
They told Miss D that her banking apps needed to be reinstalled, and they instructed her to delete them.

Within the hour, four payments – electronic transfers – were made from Miss D's Think Money account through its banking app which was accessed on a different device. Miss D became suspicious when she heard the television in the background from the caller's side, and she ended the call. She discovered money had been transferred into her Think Money account from her account with another firm, before being sent on to a third party.

Think Money attempted recovery, but no funds remained in the beneficiary account. It reviewed Miss D's claim and concluded that she'd shared secure information with the caller and this gave them access to her account. Think Money considered Miss D's actions amounted to gross negligence and therefore it wasn't liable to refund her loss. But it did refund the last payment as it felt it could have taken additional steps by the time that payment was attempted, and this could have limited her losses.

The complaint was referred to our service and when our investigator contacted Miss D, she said she couldn't remember if the caller asked her for any codes as it happened so quickly. Miss D said she didn't share the one-time passcode (OTP), which would have been needed to gain access to the Think Money app, with the caller. But she could have shared the six-digit code that she uses to log on to it.

The investigator thought that on balance its likely Miss D shared both the OTP and the six-digit code with the caller. But as she didn't complete the steps required to make the disputed payments, the payments were unauthorised. The investigator recommended Think Money to refund the remaining disputed payments along with interest.

Miss D accepted the investigator's conclusions but Think Money didn't. In summary, it submits that Miss D claims she didn't provide the OTP to the caller but hasn't provided a point of compromise (of her security credentials). So, if it wasn't Miss D who carried out the transactions, then it must be someone known to her.

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 agree with the conclusions reached by the investigator. I'll explain why.

The relevant law here is the Payment Services Regulations 2017 (PSRs). In simple terms, the starting point is that Miss D is responsible for authorised payments, and subject to certain exceptions Think Money would generally be liable for unauthorised payments.

To consider a payment authorised, the PSRs explain that Miss D must have given her consent to the execution of the payment transaction – and that consent must be in the form, and in accordance with the procedure, agreed between her and Think Money.

In their view, the investigator set out what they considered were the likely steps involved in making electronic transfers from Miss D's account (i.e., logging into the app, going to 'Payments' section, adding new payee details, etc.). Think Money hasn't disputed that finding, so I've proceeded on that basis.

I acknowledge that Miss D has previously denied sharing the OTP with the scammer. When things aren't clear, I must decide what happened based on the balance of probabilities – in other words, *what's more likely than not* to have happened. Here, there's no other plausible or persuasive explanation for how someone could have managed to access Miss D's account on the Think Money app without Miss D's involvement. That's not to say that she understood what her actions meant. Give our experience with dealing with similar scams, I find it more likely than not that she was tricked into disclosing the OTP. I note she's already accepted it's likely that she disclosed her six-digit login code.

But even with this conclusion that Miss D must have been involved in the scammer gaining access to her account, I'm not persuaded that the disputed payments were authorised.

This is because I'm satisfied that Miss D didn't complete the steps that would have been required to make the disputed payments (previously set out by the investigator). The scammer completed those steps after they accessed Miss D's account through the Think Money app on their device. And they did this using the information they convinced Miss D to share by deceiving her into believing they were from Think Money, and they were helping her secure her account.

Miss D can still be held liable for unauthorised payments if she acted fraudulently or failed with intent or gross negligence to comply with the terms of the account or keep the account security details safe.

There's been no suggestion that Miss D acted fraudulently. Or that she failed with intent to comply with the terms of the account or keep the account security details safe. Think Money has said it believes that Miss D failed with gross negligence to comply with the terms of the account and keep her personalised security details safe. In addition to sharing the codes, Think Money says Miss D ignored warnings previously given when she's logged on to her banking app. It's also explained that for someone to gain access to the Think Money app, they must be aware of the customer's account number, date of birth and email address.

Miss D says the scammer already knew her account details and some of her personal details when they called. It's unclear how these details were compromised, but there's nothing to suggest that she shared them during the call. So, I think it's more likely they were compromised beforehand – for example, through a data leak, phishing link or malware.

But I've concluded that Miss D shared her six-digit login code and the OTP with the scammer during the call. So, I've gone on to consider whether her actions mean that she failed with gross negligence.

It's not clear exactly how the scammer convinced Miss D to disclose the codes. But, given our experience of scams like this, and that we know the context of the call was that her account had been hacked, I think it's likely Miss D thought she was protecting her money.

I'm also mindful that Miss D had been presented with a worrying scenario – that there was fraudulent activity. I've reflected on Miss D's panic and trust in the caller, as well as how, like most people, she wasn't an expert in fraud. Taking all this into account, I can understand how the situation seemed plausible at the time, and why she followed their instructions, believing she was doing the right thing to protect her account.

I recognise there were warnings in Think Money's message containing the OTP as well as on its banking app. And of course, with the benefit of hindsight, it's possible to criticise Miss D's actions given these warnings. But here, Miss D was acting in the heat of the moment, panicked about fraud. In these circumstances, I can understand how she could have overlooked the overall content of the text message and simply focused on following the caller's instructions. Similarly, when she believed she needed to act hastily, I can see how Miss D didn't recall in the moment previous warnings she'd been given in the app.

In this light, I don't think that Miss D's actions in the heat of the moment fell so far below what a reasonable person would have done that it would be fair to conclude she failed with gross negligence.

So, I conclude that she isn't liable for the transactions and Think Money needs to put things right – by refunding the remaining loss from these unauthorised payments alongside interest to compensate her for the time she's been out of pocket.

Putting things right

To put things right for Miss D, Think Money Limited needs to refund the remaining disputed transactions from 20 February 2024, i.e., the first three payments which add up to £3,600.

Think Money Limited also needs to pay interest at 8% simple per year on this amount, calculated from the date of the unauthorised payments to the date of settlement (less any tax lawfully deductible).

My final decision

For the reasons given, my final decision is that I uphold this complaint. I direct Think Money Limited to put things right as set out above.

Under the rules of the Financial Ombudsman Service, I'm required to ask Miss D to accept or reject my decision before 17 September 2025.

Gagandeep Singh
Ombudsman