DRN-5783052

The complaint

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

What happened

In October 2024, Mrs J received a call from a scammer impersonating Think Money's fraud department. They asked Mrs J if she'd set up a direct debit, and whether she'd attempted a card transaction. She said didn't recognise either activity. Under the guise of securing her account, the scammer persuaded Mrs J to share a one-time passcode (OTP) as well as her Think Money app passcode. The scammer was able to gain access to Mrs J's account on a new device and make two transfers totalling £3,407.17. Mrs J subsequently realised she'd been scammed and reported the matter to Think Money.

Think Money declined to refund the payments. It said Mrs J had shared secure information and ignored warnings sent to her. Think Money also said that it contacted the beneficiary account provider, but it was unsuccessful in recovering Mrs J's funds.

Unhappy with Think Money's response, Mrs J made a complaint and later referred it to the Financial Ombudsman Service. Our Investigator concluded that the payments weren't authorised by Mrs J, nor had she failed in her obligations (to keep her security details secure) with intent or gross negligence. They recommended a full refund along with interest.

Think Money disagreed with the Investigator's conclusions. It said it provided Mrs J with warnings not to share OTPs and passcodes, including with Think Money. It said she should have done more to read the warnings and contact it.

As an agreement couldn't be reached informally, Mrs J's complaint has come to me for 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.

Having done so, I've reached the same conclusion as the Investigator for similar reasons.

Think Money has said Mrs J was negligent in sharing the secure information she did and that the following was needed by the scammer to set up access to her account on a new device:

- Mrs J's customer account number, date of birth and email address
- Mrs J's personal 6-digit passcode to enter the Think Money app
- An OTP sent to Mrs J's registered mobile number

The relevant law here is the Payment Services Regulations 2017 (PSRs). These set out situations in which Think Money can hold Mrs J liable for unauthorised transactions. Of relevance here is the obligation on Mrs J to *"take all reasonable steps to keep safe*

personalised security credentials relating to a payment instrument or an account information service". Under the PSRs, Think Money can hold Mrs J liable for the payments if they were made as a result of her failing in this obligation with intent or gross negligence. This is reflected in the applicable terms and conditions of Mrs J's account.

Think Money has suggested that Mrs J was negligent in sharing the secure information she did, and the follow-up messages it sent her should have prompted concern and action.

When considering if Mrs J has failed in her obligations with gross negligence, the test isn't simply whether she was careless. For someone to fail with gross negligence they would need to have seriously disregarded an obvious risk, falling significantly below the standards expected of a reasonable person.

I've considered the circumstances in which Mrs J shared the information that she did – she's explained that she noticed that the call came from a London phone number which was unusual, and the caller advised her that Think Money's fraud department was based there. Mrs J also recalls being asked to confirm her name, date of birth, and first line of address as part of completing security – and this persuaded that the caller was genuinely from Think Money.

After verifying some transactions with her, the caller told Mrs J that her account was at risk and that she needed to share the OTP they were sending her to block her account. When she was also asked for her passcode as part of this activity, Mrs J challenged the caller. She was told it was needed to fully secure the account. To prove to her that they were calling from Think Money, the caller said they'd send another OTP to her phone to read back to them. I think what Mrs J was told was plausible in the circumstances.

Mrs J received an OTP as expected and, believing in that moment that the caller was genuinely from Think Money, she shared the OTP. Mrs J says she didn't recall her passcode and the caller said it needed resetting. She remembers being asked and telling them what she wanted her new passcode to be, but it seems Mrs J was tricked into resetting the passcode on her own device before disclosing it to the scammer.

Given the nature of the information Mrs J shared, there is an argument to be made that she was negligent in doing so. But I don't think her actions amount to gross negligence in the circumstances. Unfortunately, scammers can utilise social engineering techniques to create a sense of panic and trick their victims into thinking they need to act to protect their funds. And it is in this context, believing she was speaking to Think Money, that Mrs J didn't read the full content of the OTP and shared this information and her passcode.

Think Money says that Mrs J had additional time after the scam call to reflect on it and the notifications it sent her before the disputed payments took place. It says she should have done more to protect her account such as call it. Think Money has shown that in addition to the OTP messages, it also sent Mrs J notifications of a new device being added. Mrs J does remember reading Think Money's notifications, but this was after the call with the scammer had ended. She's told us she thought these messages related to the fraudulent activity Think Money had just flagged to her and managed to stop.

As for Think Money's argument that Mrs J remained concerned about her money, enough to move £1,000 from her account when it was supposedly blocked, I can see Mrs J has explained that the caller told her she needed to wait up to 24 hours before she could make transfers from her account. Think Money will note that the £1,000 transfer was made 24 hours after the scam call.

As such, there's no evidence to support that Mrs J realised the call she'd had with the scammer wasn't genuine until after the disputed payments were made. Importantly, any messages or notifications Mrs J received after she had shared the secure information wouldn't be relevant to whether she acted with gross negligence at the time of sharing it. So, while I accept Mrs J could have done more to mitigate her losses, it doesn't mean that Think Money can reasonably hold Mrs J liable for the unauthorised payments – and it is required to provide a refund under the PSRs.

Putting things right

As I've concluded that the payments weren't authorised by Mrs J and she didn't fail in her obligations with gross negligence, Think Money Limited should provide a full refund to Mrs J and pay her interest (less any tax lawfully deductible) to reflect the time she's been without her funds.

My final decision

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

Under the rules of the Financial Ombudsman Service, I'm required to ask Mrs J to accept or reject my decision before 13 March 2026.

Gagandeep Singh
Ombudsman