DRN-5822509

The complaint

Mrs L complains that Think Money Limited trading as thinkmoney has declined to reimburse a payment made as part of a scam.

What happened

In December 2023, Mrs L received a call from a scammer impersonating thinkmoney. She was persuaded that fraud was occurring on her account. Under the guise of security questions Mrs L shared personal information. Mrs L is disputing one payment of £4,400.

Thinkmoney declined to reimburse Mrs L on the basis that she had shared secure information used by the scammer and ignored it's warnings. It says that an OTP (one time passcode) that it had sent to Mrs L was used alongside personal information to set up its app and access her account on a new device. And that a faster payment was then made using this new device. But it was able to recover £39.25 after being made aware of the scam.

When Mrs L referred her complaint to our service the investigator didn't uphold it – in summary they thought it was fair to treat the payment as authorised and that they wouldn't have expected thinkmoney to have intervened in the circumstances. They thought thinkmoney had done everything it needed to in regards to recovering Mrs L's funds.

Mrs L's professional representative didn't accept the outcome, in summary they said the transaction was significantly higher than previous activity on the account and that thinkmoney ought to have intervened which it says would have prevented the loss.

As an agreement couldn't be reached, the matter was passed to me for consideration by an ombudsman. I issued my provisional decision on 5 September 2025 explaining why I intended on upholding the complaint and awarding 50% of Mrs L's loss, plus interest.

Mrs L's professional representative confirmed she accepted this outcome. Thinkmoney confirmed receipt of my provisional decision and that they had no further comments.

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.

As no further information has been received since I issued my provisional decision, my findings remain that I uphold this complaint.

Has thinkmoney acted fairly in treating the disputed payments as authorised?

Under the relevant law - the Payment Services Regulations 2017 (PSRs) – the starting point is that Mrs L is liable for payments she authorised and, subject to certain exceptions, thinkmoney is liable for unauthorised payments.

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.

It's common ground that Mrs L is the victim of a scam and that she understood she was speaking to thinkmoney in relation to fraud on her account. Mrs L has been consistent that she shared personal information believing she was undergoing security.

There appears to be some dispute now about whether Mrs L shared an OTP that was used by the scammer to set up the banking app on a new device – on balance I'm persuaded that Mrs L did share this with the scammer. This is because Mrs L disclosed doing so during a call with thinkmoney on the day of the scam – and said she had done so believing the caller had sent the message to her and she needed to give them access to secure her account. Mrs L's professional representative also initially said she had read out the message to the scammer. So while Mrs L now doesn't recall sharing the code, given what she's previously said and that it was used by the scammer with no other explanation for how they could have obtained it (as no remote access was in place) I find this the most likely explanation.

In order to set up the banking app on a new device, the scammer would have needed to use some personal and contact information for Mrs L – given the overlap between the information needed and the security questions Mrs L recalls being asked, the scammer likely obtained any information they didn't already have during the artificial security process. Thinkmoney has explained that once the app was set up, the user would also need to use Mrs L's six digit passcode or (if bypassed) an OTP and Mrs L's password to access her account using the app. Thinkmoney has provided evidence of the new device being set up and the logins on that device used to set up a new payee and make the payment. So, while Mrs L doesn't recall sharing this sensitive information, as there's no other explanation for how this could have been obtained, I'm persuaded that it's more likely than not that she was also tricked into sharing this further sensitive information.

Mrs L has been consistent in saying that she thought the caller was thinkmoney and that they needed to access her account to secure it. I don't think the steps Mrs L took, or her understanding of the matter, amount to her consenting to a third party making any payments on her behalf. So, I don't think it would be fair to treat any of the payments as authorised.

I appreciate the level of authentication may have made the payment appear authorised to thinkmoney, but I don't think it would be fair to treat the payment as authorised on this basis. Thinkmoney's own warnings shown to Mrs L on the day of the scam and educational scripts read to Mrs L at the time of reporting the scam indicate that it was aware of these types of scams at the time. Businesses like thinkmoney should be aware that authentication alone is not sufficient to treat a payment as authorised. I note thinkmoney does appear to have accepted the payment was unauthorised and has held Mrs L liable on the basis that she was careless in sharing the secure information she did in the circumstances.

<u>Is there any other reason why it would be fair for thinkmoney not to provide Mrs L with a refund?</u>

The PSRs set out situations in which thinkmoney can hold Mrs L liable for unauthorised transactions. Of relevance here is the obligation on Mrs L to *"take all reasonable steps to keep safe personalised security credentials relating to a payment instrument or an account information service".* Under the PSRs, thinkmoney can hold Mrs L liable for the payment if it was 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 L's account.

Thinkmoney has said Mrs L was careless in sharing the secure information she did and it has highlighted as context that she was the victim of a similar scam previously and warnings

that were shown to her at the time. So I've considered whether Mrs L has failed in her obligations with gross negligence.

When considering if Mrs L 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. But I do think, in the circumstances, that Mrs L can be held liable on this basis, I'll explain why.

- I can appreciate why Mrs L initially thought the caller was from thinkmoney as the scammer appears to have been able to make it look like they were calling from its number. But as Mrs L had previously been the victim of a scam where the scammer impersonated thinkmoney, in addition to receiving scam education, thinkmoney had put in place a password on Mrs L's profile that it could share with Mrs L to verify that it was genuinely thinkmoney that she was speaking to. Here, Mrs L accepts she was aware of this process and says she asked the scammer for the password but they didn't provide it. Mrs L says she was told they needed to access and secure her account first but that she asked multiple times and was concerned. Based on this, I don't think the reasonable person in her circumstances would have accepted they were speaking to thinkmoney upon receiving a call from someone without this password.
- Mrs L also initially explained that she shared an OTP with the scammer believing her account was at risk and that the caller needed access to her account to secure it. She has denied sharing further passcodes/ passwords but I've explained above why I think it's likely that she did share one of these to enable the login to her account by the scammer. While this has the hallmarks of a scammer using social engineering to manipulate their victim into thinking they needed to act to protect their account, I don't think the reasonable person in her circumstances would have shared secure information such as their password or passcode (knowing their purpose) with a caller who couldn't verify themselves. Particularly if they had previously received scam education warning them of this type of scenario. Mrs L hasn't shared why she continued to believe the scammer was genuine other than the number they had called from.
- Thinkmoney has also shown that Mrs L logged into her banking app during the scam – after the scammer set up the new device but before the new payee was added or the disputed payment was made. Thinkmoney says Mrs L would have been shown a warning that said "Scam alert! 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…& call…". Mrs L says she doesn't recall seeing this message.
- The message containing the OTP that Mrs L shared said "Never share this code – hang up if anyone asks for it, including thinkmoney or the police. If you did not request this, text BLOCK to …" Mrs L says she doesn't recall sharing this code, but I've explained above why I think it's more likely than not that she did.
- Thinkmoney says that it also sent Mrs L a push notification when the new device and the new payee were set up, confirming each of these things had happened. These messages said what steps to take if it wasn't Mrs L who had set these up.
- The above warnings provided to Mrs L during the course of the scam (and before the disputed payment) did explain that Mrs L shouldn't share the codes, even with thinkmoney. I think these were relevant and should have resonated with Mrs L in the circumstances. I appreciate that scammers can put pressure on their victims to act quickly and follow instructions without question to counter the threat of fraud on their account. But in the context of what I've previously said about Mrs L's scam

experience and concerns over the caller not being able to verify themselves, I think the reasonable person in her circumstances would have taken additional care to review and follow the instructions in the warnings.
- Mrs L's professional representative has more recently said that Mrs L was concerned the scammer couldn't verify themselves but that they had somehow managed to lock her phone which prevented Mrs L from being able to come off the phone and speak to thinkmoney. This wasn't mentioned when Mrs L spoke to thinkmoney on the day of the scam, and she seemed unsure at first whether the call had been genuine. But if Mrs L did have concerns, then this would have made it less reasonable to share her secure password or passcode with the caller.
- Based on the above, I think Mrs L did seriously disregard an obvious risk and one that she had identified. And that she has fallen significantly below the standard expected of a reasonable person. So I consider that Mrs L has failed in her obligation to take all reasonable steps to keep her secure information safe with gross negligence.

I do appreciate Mrs L has been the victim of a scam and that this is an awful experience. But for the reasons explained I consider that thinkmoney can hold Mrs L liable for the payment under the PSRs.

Did thinkmoney miss an opportunity to prevent Mrs L's loss?

In broad terms, the starting position at law is that an Electronic Money Institution ("EMI") such as thinkmoney is expected to process payments and withdrawals that a customer authorises it to make, in accordance with the PSRs and the terms and conditions of the customer's account.

But, taking into account relevant law, regulators' rules and guidance, relevant codes of practice and what I consider to have been good industry practice at the time, I consider it fair and reasonable that thinkmoney should:

- have been monitoring accounts and any payments made or received to counter various risks, including preventing fraud and scams;
- have had systems in place to look out for unusual transactions or other signs that might indicate that its customers were at risk of fraud. This is particularly so given the increase in sophisticated fraud and scams in recent years, which firms are generally more familiar with than the average customer;
- have acted to avoid causing foreseeable harm to customers, for example by maintaining adequate systems to detect and prevent scams and by ensuring all aspects of its products, including the contractual terms, enabled it to do so;
- in some circumstances, irrespective of the payment channel used, have taken additional steps, or made additional checks, or provided additional warnings, before processing a payment;
- have been mindful of – among other things – common scam scenarios, how fraudulent practices are evolving (including for example the common use of multi-stage fraud by scammers, including the use of payments to cryptocurrency accounts as a step to defraud consumers) and the different risks these can present to consumers, when deciding whether to intervene.

Having considered Mrs L's previous account activity, I think the value of the disputed payment was out of character for the account. And given that the payment was also being made to a new payee on a newly set up device I think thinkmoney ought to have identified that Mrs L was at risk of financial harm from fraud.

Thinkmoney appears to be aware that scammers were asking their customers for four-digit

codes to access their banking apps. It was also aware that Mrs L was previously the victim of a banking impersonation scam.

Taking the above into account, I think thinkmoney ought to have identified a risk that it wasn't Mrs L who had made the payment. And so, it should have contacted Mrs L either on her pre-existing device or by phone to gather more information about the circumstances surrounding the payment. If it had done so, as there's no evidence to suggest Mrs L had been asked to mislead thinkmoney, I think it's more likely than not that she would have confirmed the payment was unauthorised and that thinkmoney therefore wouldn't have processed the payment. So provisionally I think thinkmoney ought to reimburse the payment on this basis.

Should Mrs L bear any responsibility for her losses?

I've explained why I think Mrs L has been negligent in sharing the information she did in the circumstances, and so I won't repeat that here.

I'm not aware of any specific vulnerability affecting Mrs L ability to protect herself at the time. I appreciate her professional representative has highlighted her age being 65 at the time. I don't think this alone would mean that it is unfair to make a deduction in the circumstances.

With this in mind, I think it would be fair to make a deduction to the amount thinkmoney pays Mrs L on this basis. Weighing the fault that I've found on both sides, I think a fair deduction is 50%.

Was there anything else thinkmoney should have done to recover Mrs L's loss?

When Mrs L reported the scam, thinkmoney blocked the newly added device and attempted to recover Mrs L's funds. It received £39.25 back and credited this to Mrs L in February 2024. In the circumstances this is what we would expect thinkmoney to do and so I don't think it needed to do more to recover Mrs L's funds.

Putting things right

As Mrs L has received £39.25 back, her outstanding loss is £4,360.75. For the reasons explained, I consider thinkmoney should reimburse 50% of this amount.

Thinkmoney should also pay Mrs L interest to reflect the time she was without these funds.

My final decision

My final decision is that Think Money Limited trading as thinkmoney should do the following:

1. Reimburse Mrs L 50% of her outstanding loss.
2. Pay Mrs L simple interest at a rate of 8% per annum on this amount from the date of the payment to the date of settlement.

If Think Money Limited considers that it's required by HM Revenue & Customs to deduct income tax from that interest, it should tell Mrs L how much it's taken off. It should also give Mrs L a tax deduction certificate if she asks/ask for one, so she can reclaim the tax from HM Revenue & Customs if appropriate.

Under the rules of the Financial Ombudsman Service, I'm required to ask Mrs L to accept or reject my decision before 15 October 2025.

Stephanie Mitchell
Ombudsman