DRN-5301801

The complaint

Ms C complains that Think Money Limited ("Think") failed to refund transactions she didn't recognise.

What happened

Ms C explained that whilst on a break from her work she checked her Think app on her phone and noticed a number of payments had left her account that day (28 November 2023) leaving her with a nil balance. Ms C didn't recognise any of the payments which had been made to a well-known financial business I'll refer to as P.

Ms C contacted Think about the situation and told them she'd been working and hadn't made the transactions herself. Ms C confirmed she hadn't received any unusual calls or requests for information or been asked to do anything relating to her Think account.

Ms C also confirmed only she knew the login details to her account and hadn't passed these on to anyone else. Think advised they'd be in touch within 15 working days as they needed to investigate what had happened.

Ms C had to ask family and friends to assist her with temporary financial help because she'd just been paid and didn't have any funds in her account due to the disputed transactions. Ms C explained that she made numerous attempts to obtain updates from Think and eventually made a complaint about their conduct on 11 December 2023. Think sent updates to Ms C to advise her they were still investigating and tried to get in touch by phone in mid - January. They eventually got in touch with Ms C on 25 January 2024, some two months after the loss of her funds to further discuss the complaint. Another conversation was held the following day and Think didn't think they could assist as there was no evidence of a compromise of her account.

Think's investigation concluded that the disputed transactions were made using a different device to the one Ms C had registered with them. This had been added to the account some days earlier after sending a code to Ms C's phone.

Think issued their final response to Ms C's complaint on 30 January 2024, accepting they'd delayed their investigation and paid £30 to Ms C to recognise their level of customer service. They didn't accept they needed to refund the transactions as they couldn't identify how the payments could have been made without Ms C's personal logon information. They also advised a One Time Passcode (OTP) was necessary to activate the account on another device and this could only have been sent to Ms C's registered phone which she was still using. Overall, Think didn't accept there was a plausible reason to show how an unauthorised third party could access the device.

Ms C was unhappy with Think's decision and the way they handled her situation, so she brought her complaint to the Financial Ombudsman Service for an independent review where it was assigned to an investigator.

Both parties were asked to provide information about the situation. Ms C was able to confirm

her earlier account she'd given Think. Ms C also confirmed that her phone had both biometric and passcode protection only she knew. She was also concerned that the loss of funds had caused her many difficulties and she'd been unable to work. Ms C explained she was in a difficult position financially and Think's decision had caused her considerable distress. She was also unhappy with the way they handled her complaint.

Think provided some details about the complaint, essentially arguing the same case they provided to Ms C, which was that:

- Ms C was unable to provide any explanation how someone else could have obtained her details to register another device, including her personal information and password.
- The disputed transactions were made from the new device.
- Ms C's passcode was used to log in to it and an OTP was sent to her registered mobile phone.
- No details were reset.
- The transactions must have been carried out by Ms C or someone known to her.
- They'd asked Ms C for evidence of message logs which weren't provided.

After reviewing the evidence, the investigator concluded that Think hadn't conducted their own investigation in a timely manner. References were made to the Think's obligations to undertake investigations within a certain timeframe. It was also recommended that they refund Ms C (including interest) as Think hadn't sufficiently proven that Ms C was responsible for the disputed transactions and there was no evidence she'd received the OTP which was critical in setting up the app on a different phone.

Overall, it was recommended that Think make a full refund and pay a further £170 for the unnecessary distress and inconvenience caused to Ms C by Think's handling of her complaint.

Think disagreed and argued they'd investigated the matter within the relevant timeframes although they accepted they'd not completed it sufficiently quickly and thought their £30 payment was appropriate. They also made further comments:

- It's impossible for someone to gain access to their app without specific information known only to Ms C, including a six-digit passcode for the app and personal details related to Ms C including name and email address.
- The new app could only be successful if the OTP code sent to Ms C's phone was used to register it.
- Evidence of four text messages from Think (OTPs) to Ms C's phone were provided.

Think requested a further review of the complaint which has now been passed to me. As part of my own investigation, I wanted to better understand the activity of both Ms C's original device and the new device. Think provided further data which showed:

- The new device was registered shortly after text messages (OTPs) were sent by Think on 25 November 2023.
- The new device logged an IP address from a different location to Ms C during registration.
- The new device used Ms C's passcode to log in then used biometrics.

- The new device regularly logged into the account over the next few days.
- The evening before Ms C received her salary into the account, the new device logged on several times to cancel several direct debits and amend available spending.
- Early the next morning, Ms C received her salary and both Ms C's original device and the new device logged in several times.
- The new device set up a new payment to P using a "friend or family" description on the same day the salary was paid in and sent seven payments totalling £2,782.30 emptying the account.
- The new device logged an IP address from a different location to where Ms C lived/worked.
- Ms C logged in about an hour after the last disputed transaction and reported the issue to Think who blocked the second device.

I also asked Ms C some further questions. In summary Ms C said:

- She had no record of any text messages but was able to provide call logs for the period.
- At the time she was living with a close relative, but they didn't have access to her phone. Coworkers also didn't have access or know the phone's passcodes which was also biometrically protected.
- No one else had access to her device on the day the new one was registered. Ms C said she was at work at the time.
- Ms C didn't know anyone from the location (a different part of the UK) logged by the new device.

Enquiries about the disputed transactions were made with P. Unfortunately, they were unable to provide any details about the account that received the funds.

I issued my provisional findings on the merits of Ms C's complaint on 31 December 2024. In my provisional findings, I explained why I didn't intend to uphold Ms C's complaint and offered both sides the opportunity to submit further evidence or arguments in response. An extract of that decision is set out below and forms part of this final decision:

"What I've provisionally 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 was sorry to hear that Ms C has experienced both financial and personal difficulties as a result of this issue. The crux of this complaint centre's around the authorisation of the disputed transactions. Ms C denies having any knowledge of them. On the other hand, Think believe that they couldn't have happened without the OTP and Ms C's passcode (amongst other details) being known by the operator of the new device. They believe that a scam was the reason for the payments. Scams and "unauthorised" complaints are dealt with differently.

Given the evidence provided by Ms C, this complaint has so far been treated as an issue of authorisation, rather than as a scam. Ms C would likely be held liable for the payments if the evidence shows she allowed access to her account, thereby providing "apparent authority" for someone else to use it.

The relevant law surrounding authorisations are the Payment Service Regulations 2017. The basic position is that Think can hold Ms C liable for the disputed payments if the evidence suggests that it's more likely than not that she made them or authorised them. But, Think cannot say that the use of the app for internet banking payments conclusively proves that the payments were authorised.

Unless Think can show that consent has been given, it has no authority to make the payment or to debit Ms C's account and any such transaction must be regarded as unauthorised. To start with, I've seen the bank's technical evidence for the disputed transactions. It shows that the transactions were authenticated using the payment tools issued to Ms C.

It's not my role to say exactly what happened, but to decide whether Think can reasonably hold Ms C liable for these transactions or not. In doing so, I'll be considering what is most likely on a balance of probabilities.

In order to register a new device (which then undertook all of the disputed transactions), certain pieces of information were required. They included Ms C's name, email, app passcode and the unique OTP sent to her mobile phone by Think just prior to the new device's registration. Without those details, it isn't plausible for someone to just guess that information.

Ms C doesn't remember receiving any OTPs to her phone and she also confirmed she didn't pass them on to anyone (which she couldn't have done if she never remembered receiving them). But, Think's evidence shows four separate OTPs were sent to her phone just prior to the new device's registration. It's difficult to imagine a plausible scenario that can explain how someone else obtained those details independently. There's no evidence that I've yet seen that could explain how this was done remotely without Ms C's knowledge. Ms C hasn't said there were any other issues with her device (it's possible to take over a device, but this would probably be apparent to the legitimate user) or any other explanation concerning how someone could have obtained her details, including her six-digit passcode for the Think App. I do acknowledge that some of the details needed to login (name/email address) could be obtained by other means (without Ms Cs knowledge).

The evidence from the IP address indicates the new device was using a location far away from Ms C. I accept that this data can be manipulated, but here it seems to discount that someone close to Ms C was responsible. That's also because if it was someone close to Ms C, they could have simply made the payments using her own phone (because whoever ultimately made them knew all the details to log into the account), rather than going to the extra step of registering a new device and possibly alerting her.

I'm currently minded to say Think have shown that the transactions were the result of a new device that was registered after information known only to Ms C was used to set it up on her account. But, I've also considered the overall picture and I accept there are some aspects to it that indicate other parties were involved, particularly the different location and the way the payments were made away from the account. But, as I can't reasonably explain how the device was registered without Ms C's knowledge, I'm unable to currently say that Think should be responsible for a refund. Of course, if Ms C is able to provide additional information that she may have forgotten or not thought relevant, this could change my thoughts on her complaint.

I appreciate this will not be good news for Ms C, but I hope she understands that I have to make my decision based on the available evidence. Essentially, the evidence points to another party being involved, but it's unlikely that could've happened without Ms C's knowledge. I don't think for one minute that Ms C thought she was going to lose those funds, but without stronger evidence to the contrary, I can't reasonably come to a different conclusion.

So, taking everything into account, my current thoughts are that I think it's both fair and reasonable for Think to hold Ms C responsible for these transactions.

I've also considered Think's handling of the complaint. Whilst it no doubt could have been done more efficiently, and Think accept they let Ms C down, I'm satisfied their £30 payment was a reasonable way for them to compensate Ms C.

My provisional decision is that I currently intend not to uphold this complaint."

I invited Ms C and Think to give me any more evidence and information they wanted me to consider before issuing my final decision. Think didn't add anything further and Ms C provided further details from her phones call/text logs and confirmed she'd reported the matter to Action Fraud. She commented that Think should've stopped those payments because she never used her account in this way.

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, and as neither party had anything further to add that would change my recommendations about this complaint, I see no reason to reach a different conclusion. So, this final decision confirms the findings set out in my provisional decision.

I realise this will be disappointing news for Ms C and I understand the removal of the funds has caused her difficulties along with other issues she's been dealing with.

I've thought deeply about her complaint and examined all the evidence to ascertain how someone could have done this without being provided with her account security details and access to her phone. My role here is to be impartial, so I can't ignore the evidence provided by Think. This shows the OTPs sent to Ms C's registered phone were then used, along with her logon details, to register a new device on her account which was then used to move the funds.

If there was any evidence that these details were somehow obtained by unauthorised third parties, for example the new device forced a passcode change after being registered (indicating they didn't know the passcode), I would most likely have reversed my decision. I appreciate this will be of little consolation to Ms C, but I'm unable to see how those funds could have been moved without those security details being passed to whoever used the new device.

I acknowledge what Ms C has been told concerning Think's obligations to detect fraud. It's accurate to say they should monitor accounts for suspicious and unusual activity. But, even if believed Think should have intervened at some point, I'm not persuaded they could have stopped those transactions. That's because I've already concluded that access to the account couldn't have been obtained without information known only to Ms C and there's a continued lack of clarity over the arrangement to use the account. So, on balance, I don't think I could fairly require Think to make a refund.

My final decision

My final decision is that I do not uphold this complaint.

Under the rules of the Financial Ombudsman Service, I'm required to ask Ms C to accept or reject my decision before 2 March 2025.

David Perry
Ombudsman