

The complaint

Mr H complains that Starling Bank Limited (“Starling”) failed to refund a transaction he didn’t recognise.

What happened

Mr H explained he was abroad and sat outside a restaurant when he noticed his phone was gone from beside him. One of his friends saw the person with the phone and it was retrieved. Later that morning, Mr H noticed a faster payment (bank transfer) had been made into an account of someone who he didn’t recognise. The transfer was for £1,000 and took place while he was at the restaurant.

Mr H notified Starling about the issue and mentioned to them that some weeks earlier, he’d had another phone stolen which had been reported. Starling cancelled Mr H’s card and issued a replacement.

Mr H confirmed to Starling that he didn’t know how someone could have obtained his passcode/password for his account. He confirmed he hadn’t written those details down anywhere. He said that he’d accessed the Starling app a few minutes before he noticed it was gone. During the initial report, Mr H said he believed the person had his phone for a couple of minutes, but later clarified it was only about 30 seconds. Mr H believed this person may have been responsible for making the unrecognised transaction.

In a later call, Mr H said to Starling that he didn’t think his app was open or that the person who grabbed his phone was able to make the transfer in the time he had it. Mr H thought that the loss of his other phone some weeks earlier was linked to the unrecognised payment. He also reported some card payments (which had been declined) had been attempted using his card.

Starling reassured Mr H that that his card was blocked, but the blocked transactions would appear on his app to keep him advised of what was happening. After reviewing the matter, Starling couldn’t find any point of compromise that could explain how the payment was carried out. Starling confirmed the unrecognised transaction was made using the phone Mr H had with him whilst abroad (and not the earlier stolen phone). Starling declined to make a refund for the loss reported by Mr H.

Mr H was unhappy and complained about their decision to decline him a refund. Mr H also believed the card payments that he’d reported were made using his new card. Starling reviewed their investigation and didn’t change their position. They advised Mr H that the card payments were attempted using an old (cancelled) card. Mr H then brought his complaint to the Financial Ombudsman Service for an independent review. An investigator was assigned to look into the complaint and asked both parties for information about the issue.

Mr H was able to confirm his version of events and that he hadn’t carried out the transaction. Starling provided details of the account including device identifiers linked to the registered phones (historically) on Mr H’s account. Additional details about the use of the Starling app and various security steps were also provided.

An initial review was made where the investigator recommended refunding the loss to Mr H because details about certain security steps weren't provided by Starling. Further evidence was provided and after receiving those details, the investigator thought that it was unlikely that anyone else was responsible for making the payment. That was because an additional password was entered at the time of the payment which was known only to Mr H. The investigator concluded that Starling hadn't acted unfairly and Mr H's complaint wasn't upheld.

Mr H disagreed with the investigators outcome. He argued that he was the victim of a scam and wasn't aware of making any payment. He thought Starling had a greater duty to protect him from scams because he'd already been a victim when his (other) phone was stolen.

The investigator responded to Mr H's further points and advised that he wouldn't be considered as a victim of a scam as he hadn't explained how he may have been deceived into making a payment. The investigator confirmed the payment Mr H disputed was made from his new phone and not linked to the theft of his old one. Mr H was also advised that the payment would have been unlikely to trigger Starling's fraud detection systems.

Mr H argued that as he hadn't knowingly authorised the payment and there's no plausible reason that a thief could obtain the relevant passwords, it can only be concluded that he was deceived. Mr H believed Starling should requested the details of the beneficiary and reported them to the authorities. Mr H also explained that the matter had caused him a significant amount of stress.

As no agreement could be reached, the complaint has now been passed 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.

I'd first like to address Mr H's comments about being deceived into making a payment which he considers should be dealt with as a scam. Having reviewed the evidence in this complaint, at no point was a scam suggested as the reason for the disputed payment by Mr H to Starling. In the context of this complaint, a scam means the payment was authorised, rather than unauthorised (which was Mr H's substantive complaint). If this was a scam, I'd expect Mr H to offer an explanation about this and accept that he had made the payment himself (for whatever reason he may have been given to persuade him to send the funds) or was persuaded to pass along certain details enabling others to use his account.

As there hasn't been such an explanation, I haven't considered this further. I have considered Mr H's complaint based on the consistent evidence he gave to both Starling and our service which is that he wasn't responsible for the payment.

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

Unless Starling can show that consent has been given, it has no authority to make the payment or to debit Mr H'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 Mr H

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

There are two thefts of phones involved with this complaint, which happened about a month apart. I think this led to some confusion when assessing the information Mr H was talking about. For clarity, Mr H had one phone stolen (Phone 1) in the UK which he never got back. That phone was the one used to try and make card payments that were declined.

The second (temporary) theft reported by Mr H took place whilst he was abroad. The phone (Phone 2) was taken from a table at a restaurant but quickly retrieved. This phone was the only phone registered to use his Starling account at that time. Mr H had earlier undertaken a specific security step to register this phone.

It was Phone 2 that was used to make the disputed transaction from Mr H's account. This payment took place about 12.15 in the morning whilst Mr H said he was at the restaurant with friends. In order to make that payment, the user had to access the Starling app, set up the new payee and confirm the payment with a secondary level password known only to Mr H.

At the time, Mr H hadn't had need to use that password which is reserved for specific security steps within the Starling app. So, it seems unlikely that anyone else could know that password and as there was no opportunity to observe Mr H enter it beforehand, I can't find an explanation that would plausibly explain how Starling's security requirements were compromised.

Mr H had told Starling that he'd earlier been using the Starling app, so it's plausible it could have been open when his phone was taken, but the thief didn't have the phone for long before it was retrieved. I think it unlikely that whoever took the phone had the opportunity or the specific security information to set up a payment.

Given that there's no plausible explanation to show how the password was entered by an unknown third party, I can't reasonably require Starling to make a refund. On balance, the evidence indicates it was more likely than not that Mr H himself either made the transaction or gave authority to others to use his device. I understand Mr H will likely disagree with my opinion here, but I have to make my decision based on the evidence and there's little to suggest that he was the victim of a scam or that the payment was somehow made by someone without his knowledge.

Regarding Mr H's assertion that Starling should have made additional enquiries, I don't think it was unreasonable for Starling to approach the dispute in the way they did. They believed the payment was made by Mr H, so wouldn't ordinarily be expected to approach the beneficiary account about the payment. I also wouldn't expect Starling to contact the authorities in this case based on that belief. Overall here, I don't think Starling acted unfairly.

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 Mr H to accept or reject my decision before 30 March 2025.

David Perry
Ombudsman