DRN-5246936

The complaint

Mr G complains that Starling Bank Limited ('Starling') debited transactions totalling approximately £1,400 from his account. Mr G says that he did not make or otherwise authorise these transactions.

What happened

The details of this complaint are well known to both parties, so I will not go into every detail of what happened here. But in summary, in February 2024 a series of transactions debited Mr G's account which he says he did not make or otherwise authorise.

The payments in question took place over three dates in February 2024, and went to numerous merchants through online card payments. There were a series of exchanges into foreign currency as part of the transactions. Mr G said that he noticed them when he went into his Starling app to see if an expected payment had gone out. Mr G got in touch with Starling to dispute the transactions. He told them that he:

- Still had his mobile device and nobody else had access to it, nor did anyone else know what his passcode for it was (though he clarified to our service that his partner knows his passcode);
- Had not received any suspicious calls, clicked on any suspicious links or provided his card details to anyone;
- Had not downloaded anything like apps or software onto his mobile around this time, and had only paid for things through official apps;
- Could not think of anything these payments could have been in connection with, and noted that they were in currencies he had never bought anything in before;
- Had been 'hacked' on an account he held with another bank around the same time, and they had refunded the disputed transactions and said there could be something on his device.

Starling looked into what happened and declined to refund the disputed transactions. They said that there was no evidence to suggest the transactions were fraudulent, and said in summary this was because:

- Mr G's testimony was that he had the device linked to his Starling account on his person at the time of disputed transactions;
- Mr G said no one other than him had access to his device; and
- The transactions were made securely using biometric or passcode authentication, and '3DS' authentication which would have been set up at the time of setting up his Starling account.

They did recognise in their final response on this matter that there were delays in their investigation and poor communication from them, so they arranged a payment of £70 in recognition of the distress and inconvenience this may have caused Mr G.

Unhappy with their response, Mr G escalated his concerns to our service. One of our investigators looked into what had happened and did not recommend that Mr G's complaint

be upheld. In summary, they could not see how the payments could have been made by someone other than Mr G or someone acting on his behalf.

Mr G said he did not agree, as he did not make the transactions. As no agreement could be reached, the case was passed to me to decide.

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 have reached the same conclusion as our investigator and for broadly the same reasons. I'll explain why in more detail.

Generally, Starling can hold Mr G liable for the disputed transactions if the evidence suggests that it is more likely than not that he authorised these payments or gave someone else consent to make them on his behalf. I am satisfied from Starling's evidence that the payments were properly authenticated – that means Mr G's genuine card details were input to make the transactions, and where required they were authenticated through the Starling app. But the regulations relevant to this case say that is not, on its own, enough to enable Starling to hold Mr G liable. So, I need to think about whether the evidence suggests that it is more likely than not that Mr G consented to these transactions being made. Having done so, I think on balance it is most likely that Mr G authorised these transactions. I'll explain why.

- It is unclear how someone other than Mr G could have had his card details. Mr G's own testimony is that no one else would have been able to access his physical card. Mr G said he did not recall receiving any texts or emails or downloading anything to his device which caused him to be suspicious. Mr G also said that he does not recall being asked to input his card details anywhere, or buying from any new or unofficial websites. So, I do not think it is likely that an unknown third party gained access to his card details by tricking him into giving them out around the time of the disputed transactions.
- The only other place I am aware of that someone could have accessed Mr G's card details would be within the Starling app itself, but it is unclear how this could have happened. I say this because and it is unclear how someone other than him could have had access to his device or got through the security measures on his device. The only other person who knew Mr G's passcode for his phone was his partner, whom he has said would not have made the disputed transactions. Whilst his passcode to get into the phone may have been something people who knew him could guess, he said his passcode for his app was a four-digit random number which no one else knew.
- The technical evidence shows that the transactions took place on Mr G's genuine mobile phone. I say this because the evidence shows that the device ID and IP address match those used for genuine transactions, and logging into the Starling app. There were no new devices added to the Starling account during the time of the disputed transactions.
- The transactions also took place on the same IP address as genuine transactions. It is true that an IP address can be shared, for example if two devices are on the same router. So, Mr G could share an IP address with anyone on the same router such as people he lives with, but given the surrounding evidence, this does not appear to be the most likely thing that happened here.
- Starling have also shown that the payments triggered additional in-app verification, which required Mr G's Starling app to be opened to verify the payments. This was also done from the same device ID and IP address as undisputed transactions and logins. This required either biometric identification, or the passcode to be entered for

his Starling app.

- So, for an unknown third party to have made these transactions, they would have had to gain access to his phone, which was pass-code protected, and his app, which was protected by a different passcode, and his card details. The disputed transactions spanned three different dates, which would seem unnecessarily risky if someone had access to all of the things needed to get into Mr G's Starling app, and make payments on his behalf. Whilst not impossible, it seems more likely that someone with access to all of those things, and an intention to defraud Mr G, would maximise their profits by quickly spending as much as they could, as they would not know if or when Mr G would notice and contact Starling and put a stop to their fraud. And taking and replacing Mr G's mobile phone would provide an additional risk to being caught.
- Mr G has suggested that his device could have been remotely hacked. Mr G has answered our service's questions, and his testimony does not provide a clear point of compromise for how someone would have managed to make transactions from his own device. Whilst this is not impossible, it is not an easy thing for an unknown third party to do, and it generally will require some granting of permissions to allow them access to the mobile phone or device. Mr G did not recall downloading any new apps, clicking on any links, or receiving any strange emails or texts. And as I outlined above, if someone had managed to do this, I would have expected them to maximise their profits in a short time scale rather than making a series of transactions over three dates. This is not to say this is impossible – but it does not seem the most likely scenario here.
- I appreciate Mr G told our service that his other bank said they refunded disputed transactions as there was something on his device. But when our service asked them about this, they did not say there was any such evidence to support there was something on his device. And whilst I appreciate the other bank did refund some disputed transactions, I'm afraid that does not impact the outcome of this case. I have considered the evidence available, including that provided by the other bank, and I simply have not been able to find evidence as to how an unknown third party could have completed the disputed transactions.

So, having considered the available evidence, I think the most likely thing that happened here is that Mr G or someone acting on his behalf made these transactions. And so, it follows that it would not be fair and reasonable for me to ask Starling to refund the disputed transactions – so I will not be requiring them to do anything further in relation to this dispute.

I also think the award Starling have already paid in recognition of the poor customer service when he reported the disputed transactions is fair and reasonable, so I will not be asking them to do anything further in relation to this either.

My final decision

I do not uphold this complaint.

Under the rules of the Financial Ombudsman Service, I'm required to ask Mr G to accept or reject my decision before 8 August 2025.

Katherine Jones
Ombudsman