DRN-5037150

The complaint

S Ltd, represented by its directors Mr and Mrs O, complained because Starling Bank Limited refused to refund the company for transactions which they said they hadn't authorised.

What happened

On 6 June 2024, eight faster payments debited S Ltd's account. They totalled £8,300. Shortly afterwards, Mr O, for S Ltd, contacted Starling by chat and disputed the payments, asking for a refund. He said his device was missing, and was taken by someone, but he didn't know who, and hadn't shared his details with anyone. He said they'd first found out when Mrs O received notifications about the payments.

Starling investigated. The next day, it contacted Mr O and said it could see that the disputed payments had been made by faster payments made on Mr S's registered device. This means that Mr S's mobile and his password had been entered to make the payments. It asked Mr O to explain how someone could have authorised these payments using his mobile device.

Mr O replied that he had no idea how the payments could have been sent from his device. Starling refused to refund S Ltd. It added that when opening a Starling Bank account, S Ltd had agreed not to share or record the security details. The terms and conditions said that Starling wouldn't be liable for losses incurred as a result of the customer's negligence, fraud or breach of any of the terms of our agreement, or losses incurred as a result of sharing information, security information or the app with any other person.

Mr O, for S Ltd, complained. He said he wasn't happy, as S Ltd hadn't made the payments. He said his phone had been in his possession when the payments had been made. He also said that they weren't normal payments.

Starling didn't uphold S Ltd's complaint. In its final response letter on 17 June, it repeated that the faster payment feature requires a customer's mobile device and password to be entered to complete the payment. Mr O's registered device had been used to make the payments. Starling said there was no evidence that S Ltd's account or login information had been compromised, so it refused to return any money.

Mr O, for S Ltd, wasn't satisfied and contacted this service.

Our investigator didn't uphold S Ltd's complaint. He said that Starling had provided online banking records which showed that the IP address (a unique computer identifier) used to make the disputed transactions was one which Mr O had used for genuine activity. And that IP address had also been used by Mr O to report the disputed transactions. Mr O's usual device had been used to make the payments. Mr O had said that his phone was password protected and still in his possession, and he hadn't recorded any of his passwords or banking details. So the investigator couldn't identify any point of compromise for Mr O's phone and S Ltd's account.

Mr O, for S Ltd, didn't agree. He asked how to appeal the investigator's decision. The investigator told him he could request an ombudsman's decision, but also said he'd reconsider if Mr O would provide an explanation about how someone else could have made the transactions using Mr O's usual device, which Mr O had later used to report the activity. Mr O replied that he couldn't offer an explanation about how anyone else could have made the transactions, because his phone had been with him. He asked for an ombudsman's 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.

There are regulations which govern disputed transactions. The relevant regulations here are the Payment Services Regulations 2017. In general terms, the bank is liable if the customer didn't authorise the payments, and the customer is liable if they did authorise them. The regulations also say that account holders can still be liable for unauthorised payments under certain circumstances – for example if they've failed to keep their details secure to such an extent that it can be termed ''*gross negligence.''*

So what I've considered is whether it's more likely than not that S Ltd, or an unauthorised fraudster, carried out the disputed payments.

I recognise that S Ltd's directors have said they didn't authorise the payments. But I've also looked at the technical computer evidence about the payments.

This shows that the payments were all carried out with the phone which was registered to S Ltd's account, which Mr O had used for genuine payments.

I've looked at the chat records, and when Mr O first reported the dispute on 6 June, he wrote in Chat: *''My device was missing. It was taken by someone. I don't know who. I've not shared with anyone.''* But after Starling refused a refund, Mr O complained on 15 June, when he said ''*I'm not happy we have not made these payments. My phone was in my possession during this period.''* So Mr O changed his evidence significantly, after Starling's initial refusal to refund. The two answers were only just over a week apart, and I think it's unlikely Mr O would have forgotten what happened in that time.

Importantly, too, the IP address used to make the disputed transactions was the same as the one used by Mr O to make genuine transactions, and by Mr O to report the dispute promptly after the transactions. So I consider it's most likely that the disputed transactions were authorised by one of S Ltd's directors. This means that Starling doesn't have to refund S Ltd.

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 S Ltd to accept or reject my decision before 21 January 2025.

Belinda Knight
Ombudsman