DRN-4427807

The complaint

Miss O complained because Bank of Scotland plc, trading as Halifax, refused to refund her for a transaction which she said she didn't make.

What happened

On 29 March 2023, Miss O rang Halifax to say there was a transaction on her account which she hadn't made. The £178.20 transaction had debited her account on 28 March and was to an online booking firm. Miss O told Halifax that she'd used that online booking firm in the past, but not for a long time. She said that she was the only person with access to her account, and no family or friends used the card. She still had her card and hadn't used any suspect websites. Halifax provided a temporary credit and investigated.

Halifax contacted the online booking firm. It replied saying it had compelling evidence that Miss O had made the transaction. It provided her name, address, email address, phone number, and the IP address (a unique computer identifier) from which the transaction had been made.

Halifax saw that the evidence provided by the online booking firm was an exact match for its own records about Miss O. It emailed Miss O on 5 April, saying it had matched Miss O's name, billing address, email address and IP address to the transaction. So Halifax said it would remove the £178.20 it had credited to her account within 10 days unless she had any further information for it to consider.

Miss O rang Halifax about the email, and asked if it was a genuine email. Halifax's adviser incorrectly told Miss O that Halifax hadn't sent her the email.

Halifax re-debited Miss O's account with the disputed £178.20 on 20 April. Miss O complained.

In Halifax's final response to Miss O's complaint, it said that the online booking firm had provided information which matched her name, home address and email address, as well as her IP address, which was the reason why the disputed amount was being re-debited. Halifax apologised that its adviser on 5 April had told Miss O that the email wasn't from Halifax and she should ignore it, which wasn't correct. Halifax paid Miss O £30 compensation for the adviser having said the email wasn't from Halifax, when it was. But it wouldn't refund her with the disputed £178.20.

Miss O wasn't satisfied and contacted this service.

Our investigator didn't uphold Miss O's complaint. She thought it was more likely than not that Miss O had authorised the disputed transaction.

Miss O wasn't satisfied. She said that the website was a slightly different address from the one which the investigator had said provided the information. The investigator explained the relationship between the two names. Miss O sent a document which she said showed her booking history for that site.

But the investigator wasn't persuaded. She said that the booking had been made from the IP address which Miss O used for her online banking. And Miss O had said her phone was password protected and no one else had access to it. The investigator said she'd seen evidence which showed that the booking had been made using Miss O's genuine information, and all details and confirmation of the booking had been sent to Miss O at that genuine contact details.

Miss O didn't agree, and 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. So I've considered whether it's more likely than not that Miss O authorised the disputed payment.

I've looked at the evidence provided by the online booking company. Its details of the disputed transaction included Miss O's name, postal address, and email address. It also provided the IP address used for the transaction. I've checked all this information against other transactions on Miss O's Halifax account, which she didn't dispute, and the details are the same. The online booking company also provided the phone number used for the booking, which matches that on Halifax's records for Miss O, and which she gave to this service.

So the disputed transaction was authorised by someone who gave Miss O's genuine name, address, email address, and phone number for the booking. It was made at her IP address.

Miss O said that her phone was protected by a password, and that she hadn't given anyone else her password or her online banking information. As I've set out above, she also told Halifax that she still had her card and hadn't used any suspect websites.

I've seen the information which the online booking company sent to Halifax. This says that the agreed price to be paid for a two-night booking for two people at the stated hotel between 17 and 19 March 2023, would be £367.20. There was a clause specifying a £178.20 cancellation fee for cancellations from 16 March onwards, and also provision for the same fee for a ''no show.'' It was this £178.20 which the online booking company, for the hotel, debited from Miss O's account on 28 March. So the evidence indicates that a booking was made using Miss O's details, and when she either cancelled after 16 March or didn't turn up, the cancellation / ''no-show'' fee was debited in line with the contract.

There's no obvious way in which any third party could have obtained Miss O's personal details, and her Halifax details, and carried out the transaction at her IP address. Miss O said she didn't carry out the transaction herself. But if she provided someone else with her personal and financial details, so they could carry it out at her IP address, it still counts as being authorised by Miss O.

I also can't see why any third party fraudster, even if they'd been able to access Miss O's Halifax account, would have made a booking where the confirmation details including the check-in voucher would be, and were, sent to Miss O rather than to the fraudster. There would have been no benefit to any such fraudster, and an obvious risk that Miss O would report it.

I'm not persuaded by Miss O's argument that the two slightly different website names mean that she didn't authorise the payment. The two are connected.

So I consider the most likely scenario is that Miss O made the booking herself, and that she either cancelled it on or after 16 March, or didn't show at the hotel, incurring the £178.20 charge in line with the contract she'd agreed.

Finally, I've considered the inaccurate information given to Miss O by the Halifax adviser on 5 April when he told her the Halifax email rejecting her claim hadn't been sent by Halifax. I find that the £40 compensation Halifax paid Miss O was fair and reasonable for this error by its adviser.

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 Miss O to accept or reject my decision before 25 January 2024.

Belinda Knight
Ombudsman