DRN-3113765

The complaint

Miss A complains that Bank of Scotland plc trading as Halifax failed to refund two transactions she didn't recognise.

What happened

Miss A explained that someone accessed her account and made two bank transfers to another account without her authorisation. Miss A called Halifax after she received a text that she'd registered for mobile banking.

Halifax blocked the account and asked Miss A to bring her identification into a branch, which she did. She was told that two payments had left her account but Miss A denied it was her that had authorised them.

Once Halifax had looked into the transactions, they believed Miss A had authorised them and declined to refund her. Miss A made a complaint and Halifax re-looked into their investigation and didn't change their position. Miss A remained unhappy and brought her complaint to the Financial Ombudsman for an independent review.

Miss A's complaint was looked into by one of our investigators who asked both parties for evidence. Miss A explained she hadn't known anything about the two payments or the person they went to. In a call to Halifax via her representative, she said that she hadn't received other texts sent to her phone about payees set up on her account or any calls about them. Miss A hadn't given her log-in details or passwords to anyone. She confirmed she'd kept her phone with her throughout the time the disputed transactions took place, so couldn't understand how they'd been made. Miss A said she'd spent some time in shared accommodation and used their facilities to access the internet.

Halifax presented audit data about a second device that registered on Miss A's mobile banking account. This device used Miss A's registered phone number and a consistent IP address throughout the transactions.

Note: IP addresses are a means to identify physical locations that online transactions are connected to and can be the actual physical location or other locations connected to the provider of the data services.

Halifax stated that security messages were sent to the new phone which confirmed the payments. Together with the security information needed to access Miss A's account, they believed she was responsible for authorising the transactions. Halifax supplied statement information showing that there were additional funds available in the account after the two disputed transactions had been made.

Our investigator thought it was reasonable for Halifax to hold Miss A liable for the two transactions and didn't uphold the complaint.

Miss A disagreed and maintained that she hadn't anything to do with the two transactions and asked for a further review of her complaint. It's now been passed to me for a decision.

I've asked Miss A for further information concerning the registration of the second mobile but haven't received any response.

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.

Coming to the question of authorisation, this is made up of two parts. Authentication and consent. Authentication is usually referred to as the technical information about the transactions. Halifax have supplied that evidence and I'm satisfied it shows the disputed transactions were authenticated.

Consent is a formal step in the payment process and refers to the way in which Halifax and Miss A agreed to operate the account. For example, when using the security details to log in to Halifax's mobile app, Halifax agree to accept that this is a legitimate payment instruction made by the account holder or another approved user and make the payment on their behalf.

Because the transactions in this case have been shown to be properly authenticated and they used Miss A's security details to log in to her account - I'm satisfied that consent was given, and the disputed transactions were authorised. But, there are exceptions where it wouldn't be appropriate for Halifax to hold Miss A responsible, for example if the card was used without her permission.

Miss A has reported that the first she was aware of a problem was when she saw a message from Halifax about a new payee set up on her account. Halifax confirmed that they'd registered a new device prior to the new payee being set up using Miss A's mobile phone number, which had logged in to her account using her security details.

Halifax's system sent a message to Miss A's registered phone about the new device and the new payee and received confirmation which allowed the device to be set up and the payments to leave her account. Miss A has denied it was her who set up or sent these payments and believes it was someone else who was responsible.

I've examined the information surrounding the payments and what happened to Miss A's online account. Halifax's records show that two devices attempted to login to Miss A's mobile banking app within a couple of minutes of each other. The second device was registered on Miss A's account just prior to the disputed transactions taking place. This triggered a message to Miss A's phone and the system records show that confirmation was received. Further confirmation was recorded when the new payee was set up. So, Halifax had registered a new device and made payments after receiving appropriate confirmation from Miss A's mobile phone that was used to access Halifax's mobile banking app.

In order for someone unknown to Miss A to have done that, they would have needed other private security information from her and access to her mobile phone without her knowledge. Miss A has said she was on a trip when this happened and her phone was with her. I've asked Miss A about the second phone but haven't received any explanation from her about it. So, it seems unlikely that an unknown third party could have acquired the relevant security information in order to access Miss A's account and used her genuine phone number to do it.

I've considered if Miss A's phone number was "cloned", which would likely divert Halifax messages to the second phone, but I don't think this is the case. That's because the same phone number was still being used by Miss A when she sent those messages to the Financial Ombudsman. I think this was because it was Miss A who was in possession of the phone at the time, otherwise the messages would have been unlikely to have been received

if they were sent to “cloned” device. The main point of cloning a phone number is to divert such messages – but the evidence here appears to show that it was Miss A’s phone that received them.

If her phone was cloned, I would have expected Miss A wouldn’t have been able to use it at all, but that wasn’t the case because she called Halifax from it later that evening. Halifax stated that the IP address was consistent with earlier undisputed use, but due to the time that’s passed that evidence is no longer available to examine.

I also examined the account when the two payments were made. There was a large balance left in the account after the two disputed transactions were made. If they were made by an unauthorised third party who had access to Miss A’s mobile banking, then they would likely have been aware of the remaining balance. I think it’s unusual that these funds were left untouched in the account. Ordinarily I’d expect any thief who had access to someone else’s account would try and take everything from it that they could, but that didn’t happen here. It would have been a simple matter to send a further payment to the same account or set up a different payee and take the remaining funds.

Of course, it’s possible that when Miss A used the shared internet facilitates at her accommodation, something happened to compromise the security of her phone and banking app, but I don’t think this is the likely explanation. That’s because Miss A received the messages from Halifax on her phone, even though her representative denied this during a call to Halifax. There were two logins using different devices two minutes apart and this seems quite coincidental if the second device was used by an unknown third party. Also, Halifax received confirmation from Miss A’s phone after sending those messages and there were funds left in the account which doesn’t follow the usual pattern of theft.

Whilst I’m sure Miss A will disagree with me, my objective assessment based on the available evidence is that I think it’s more likely than not that Miss A was responsible for making the disputed transactions or allowing others to do so on her behalf.

My final decision

My final decision is that I don’t uphold this complaint against Bank of Scotland plc trading as Halifax.

Under the rules of the Financial Ombudsman Service, I’m required to ask Miss A to accept or reject my decision before 17 May 2022.

David Perry
Ombudsman