DRN-4345716

The complaint

Mr B complains that Bank of Scotland plc trading as Halifax is holding him liable for payments he says he didn't authorise.

What happened

Mr B says he was looking for a loan online, and was contacted by a company who said they could help him find one. He had to provide identification documents as well as his card details, and thought he had obtained a £10,000 loan. But then a series of cryptocurrency payments were taken from his Halifax account. Mr B thinks the company who contacted him were actually scammers, and says they made the payments without his consent.

Halifax hasn't agreed to refund Mr B. It says many of the payments made or authorised in-app. Mr B said he had lost his phone and had since got a new one. But when Halifax asked him about a particular login after he said he'd got a new phone, which Mr B confirmed was him, it found this had been done on a device that had been connected to the account since 2021. So, it concluded the payments were authorised.

Unhappy that Halifax wouldn't refund him, Mr B referred his complaint to our service. Our investigator didn't uphold it. She wasn't persuaded by Mr B's explanation of how these payments could have been completed without his permission. She noted he had paid the same cryptocurrency merchant previously, and some payments had been authorised using biometrics on the same phone used on the account since 2021.

Mr B has appealed the investigator's outcome. He disagrees with her that the payments didn't look like fraud due to their size. I've been in touch with Mr B to find out more about previous cryptocurrency payments from his account – as there were some in the week or so preceding the disputed payments, as well as some the previous year. He couldn't remember much about the 2022 payments, but said he had been making cryptocurrency payments in 2023 after being contacted on WhatsApp.

I also asked Mr B more about his lost phone. He said he couldn't remember exactly when he lost it, he didn't make a claim as it wasn't insured, and he didn't notify his network provider.

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've decided not to uphold it. I appreciate this will be disappointing for Mr B. I've explained how I've reached this conclusion below.

Having spoken to Mr B, he has confirmed he is disputing a series of payments sent to a cryptocurrency merchant, C. But not some earlier payments, made in the weeks and days leading up to the disputed payments, to another cryptocurrency merchant (B).

Mr B says he didn't authorise the payments to C. Broadly, the starting position under the

Payment Services Regulations 2017 (PSRs) is that Mr B is liable for payments he authorises – but Halifax would be liable for unauthorised payments taken from the account.

Several disputed payments were made from Mr B's mobile banking app, or by accessing it as one of the authorisation steps. So, for an unauthorised person to have made these payments, they would have needed access to Mr B's phone and banking app.

Mr B says he lost his phone around this time. But we can see he was using his phone to make undisputed payments in the days leading up to the disputed payments. That would only leave a very narrow window for the phone to have been lost. Mr B hasn't been able to provide any corroborating evidence – such a record of reporting his phone lost or stolen, or of getting his network provider to block it – to support that it was lost at the time of these transactions.

Additionally, Halifax's records suggest only one device is registered to the account, and was used to access it for several weeks after the disputed payments. When Mr B spoke to Halifax to report the fraud, it asked him about a login the previous day and he confirmed it was him. But this was done on the same device registered to the account since 2021 – which Mr B had said he had lost and replaced by that point. So his explanation doesn't seem to hold up.

If someone had taken the phone to make these payments, they would have needed further security information to access the app. Mr B hasn't been able to account for how else someone would have been able to do this. He's suggested the transactions were made by the people who contacted him about a loan, who he says asked for his card details. But the messages he's provided don't show him being asked for these – or sharing them. Furthermore, the card details alone wouldn't have been enough to make these payments – as the app was used to verify/make several disputed payments.

It does also seem unusual that an unauthorised person would go on to make payments that were similar in nature to those made by Mr B in the days leading up to the disputed payments. He had been making payments, and receiving credits, from another cryptocurrency merchant regularly. So it seems unlikely that an unauthorised person would then make such similar payments.

I've also found Mr B had paid the merchant who the disputed payments were sent to (C) in 2022. When I asked Mr B about these earlier payments, he couldn't recall much about them. But it's another factor which raises questions. As, again, it seems coincidental that an unauthorised person would be paying a merchant Mr B had used previously, and who he may well have had an account with.

In all the circumstances, I consider it more likely these payments were authorised by Mr B. His explanations have been inconsistent at points, and they don't marry up with the information Halifax has provided about how the payments were made. In the circumstances, I don't have a plausible explanation for how someone else could have made these payments without Mr B's consent.

My final decision

For the reasons given above, 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 B to accept or reject my decision before 12 March 2024.

Rachel Loughlin
Ombudsman