DRN-4806870

The complaint

Mr W has complained that Bank of Scotland plc (trading as Halifax) won't refund transactions he says he didn't make or otherwise authorise.

What happened

In 2023, over the course of over two months, around £18,000 was spent on Mr W's Halifax account. This was a mixture of online card payments, mostly to an adult platform, and bank transfers.

Mr W says these were made without his permission. In response to questions, he explained he'd not lost his card or phone. He confirmed that he'd registered the only phone registered to the account. Only he and the close family he lived with had access to his computer. He'd not given anyone his card or security details, the only record of his security details was in a diary in a safe place at home, and his phone was strongly protected. He hadn't received any suspicious contact. No one asked him for his security details or one-time passcodes and he didn't give any out. He couldn't remember exactly what times he'd checked his account but confirmed some of the logins were most likely him. The online payments were made at the normal times he was on his computer, and he'd received emails confirming being signed up to some of the platforms involved.

Halifax held Mr W liable for the payments in dispute, on the basis that the payments had used his device and his usual IP address, as well as codes only Mr W was sent by texts or automated calls. Mr W had responded to texts to confirm disputed payments as genuine, and he'd been sent many notifications of the activity and checked his account at the time. They did pay him £50 compensation for not giving better service during a branch visit.

Our investigator looked into things independently and didn't uphold the complaint. Mr W and his family appealed, arguing that he must have been hacked somehow. The complaint's been 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.

Broadly speaking, Halifax can hold Mr W liable for the payments in dispute if the evidence suggests that he authorised them.

I'm satisfied from Halifax's technical evidence that the payments in dispute involved the use of Mr W's genuine card details and security details, his registered device, and his internet connection. The security on his account was not bypassed, I've not found any evidence he was hacked, and there are no signs of remote access. So I can see that these transactions were properly authenticated. The question, then, is whether the evidence suggests that it's most likely Mr W consented to the transactions, or not.

Only one phone was registered to the account. The model matches the model Mr W says he had. It connected to the account on Mr W's usual internet connection, using the service provider Mr W confirmed as being his. Mr W confirmed he did register his phone in that same time period, and no other phone was registered. So I'm satisfied that this was Mr W's phone. Straight after Mr W registered it – within two minutes and while still on the same connection – it began to be used to transfer funds which Mr W now says were transferred without his consent. I've not found any likely or plausible way that someone could have been using Mr W's phone without his consent at the same time he was using it himself. The only likely and plausible explanation I've found is that the transfers were authorised.

The person making the disputed payments knew Mr W's full card details, login details, and security details. But there's no sign anyone was accessing his devices remotely, Mr W confirmed he hadn't told anyone these details, the only record of them was in a safe place at home, he hadn't responded to any suspicious contact, he hadn't pre-stored his card details, and he hadn't given away or lost his card. So there doesn't seem to be a likely or plausible way that a third-party fraudster could've learned all of these details without Mr W's consent.

Further, it seems that payments to the same disputed companies continued to be made using Mr W's new details, even after Mr W made his initial fraud report, factory reset his device, had his card replaced, and had his security details changed. At that point, any details a fraudster had known would no longer work, his current details would be brand new, and the only person who would have reasonably known all those new details was Mr W.

In order to put some of the disputed payments through, codes were required, which were given to Mr W via texts or automated calls to his phone number. This was the only phone number registered to the account, and the same number Mr W gave us. So I'm satisfied this was Mr W's genuine number. As such, it's most likely that only Mr W knew the codes to put those payments through. And the codes were correctly entered. So it's most likely that Mr W consented to those payments.

Similarly, Mr W was sent text messages at that same number asking him to confirm whether since-disputed spending was his. At the time, he confirmed it was his.

The disputed spending took place at the same IP address Mr W used for his genuine activity – and continued to use after. It matches up to Mr W's service provider and his general location. Mr W pointed out that a staff member thought the IP address might be someone else's as well. Having listened to the call, the staff member seems to have been confused. It's unclear what they based their assertion on, not least as it's not generally possible for two different devices to have the exact same IP address at the same time. And as that staff member has since left, I can no longer ask them about their reasoning. As set out before, I've not found any signs of hacking or remote access. It's most likely that the staff member simply made a typo or a similar mistake when searching Mr W's details. But even if I were to accept that the IP address data was unreliable – which I've not – the other evidence still strongly supports that the disputed payments were authorised, as set out above and below.

Mr W carried out genuine activity of his own within minutes of activity he now disputes, on the same device and internet connection. For example, he paid for some student software just minutes after a disputed payment. And just minutes after Mr W registered his phone and app to the account – the only phone which was registered, which Mr W confirmed he registered himself – that very same phone was used for transferring funds which he now disputes. Again, this supports that the disputed spending was in fact genuine activity.

Mr W said he received emails confirming he'd registered to some of the platforms involved. It's not likely or plausible that a fraudster would use Mr W's real email address to sign up. If they did that, the fraudster would be unable to access key correspondence about the accounts they were trying to use, and would usually be unable to even complete the sign up process, as sites typically require one to activate accounts via a link sent by email. And it would mean that the victim would be notified of the fraud straight away and be able to prevent it before the fraudster could even spend anything. It's much more likely that Mr W's genuine email was used because the registrations were themselves genuine.

On that note, Mr W received not only emails about the disputed activity, but also many text messages letting him know what was going on. I can also see that his online banking was checked a number of times while the disputed activity was happening. And Mr W confirmed that at least some of those logins were him checking the account. So Mr W would've reasonably been aware of the disputed activity at the time, and surely would have noticed that his balance was thousands of pounds lower than before. Yet he didn't tell Halifax anything was wrong until over two months after the disputed activity started. It is not likely or plausible that Mr W would wait so long to report the disputed payments if they were being made without his consent.

While this is a more minor point, I might've expected a thief to try to take as much money as possible, as quickly as possible, before the fraud is discovered and the account is blocked. But here, the person using the account made payments far more slowly than they could have, and over a very lengthy period. This does not seem likely to have been done by a thief. It's also notable that much of the disputed spending appears to have taken place via Mr W's computer, around the times he said he was usually on his computer.

Finally, I've not seen any evidence which makes it seem implausible or unlikely that Mr W could've authorised these payments or given someone else permission to make them. And having listened to the relevant calls, I've not found any other basis on which Halifax need to pay Mr W any further compensation.

In summary, the disputed transactions were properly authenticated, using Mr W's device, card details, security details, and internet connection. Some transfers used Mr W's phone, straight after he registered it, which he confirmed he did himself. I've not found a likely or plausible way that a fraudster could've known all of Mr W's various details without his consent, not least after he changed them. Mr W received the codes used to put payments through, and confirmed payments as genuine when asked at the time. He carried out genuine spending alongside spending he now disputes. He received the signup emails for platforms he's since disputed using. He would've been aware of the activity at the time, but didn't report it until much later. And the transactions are not consistent with what I'd expect in fraud. I've not found any likely or plausible way that the payments could've been made without Mr W's consent. Instead, the evidence strongly supports that they were made by Mr W or by someone he'd given his permission to.

So I find that it's fair for Halifax to decline a refund in this case. I appreciate that this is not the outcome which Mr W or his family were hoping for. But given the evidence at hand and the balance of probabilities, I'm unable to reasonably reach any other conclusion.

My final decision

For the reasons I've explained, I do not uphold Mr W's complaint.

This final decision marks the end of our service's consideration of the case.

Under the rules of the Financial Ombudsman Service, I'm required to ask Mr W to accept or reject my decision before 9 July 2024.

Adam Charles
Ombudsman