DRN-5366070

## The complaint

Ms H complains Bank of Scotland plc trading as Halifax is holding her liable for withdrawals from her account which she says she didn't authorise.

## What happened

The details of this complaint are well known to both parties so I won't repeat them all again here. But I've summarised the events and points I consider key to my decision.

On 18 December 2023, a new device was registered on Ms H's Halifax online banking. In-app, Ms H's PIN was then viewed and her card was reported as damaged. A new one was therefore ordered to her (genuine) home address. This prompted a text to Ms H saying, *"Dear [Ms H], Thank you for ordering your new card and/or PINs. You should receive your new items within 5 working days".*

Then on 25 December 2023, the phone number registered to Ms H's Halifax profile was changed. This prompted a text to the old number, belonging to Ms H, notifying her that her phone number had been changed and asking her to call if this wasn't her. Between 27 December 2023 and 13 January 2024, a series of ATM withdrawals were made using this new card amounting to several thousand pounds.

Ms H says she didn't make these withdrawals and only found out about them in mid-January 2024 when a payment declined, prompting her to check her online banking. She then reported them as fraudulent to Halifax – mentioning she had received a call from who she had thought was its fraud team in December 2023, during which the caller went through security and she was prompted to log into her online banking. She said she was told fraud had been attempted but successfully prevented. Halifax has no record of making this call.

Halifax didn't agree to refund Ms H. It said it couldn't see how anyone else could have got access to her account, noting she said she didn't share any bank details including her login credentials – which had been used to set up the new device and order the card. Unhappy with this answer, she referred the matter to our service.

Our investigator ultimately didn't uphold Ms H's complaint. Ms H told the investigator she had in fact shared her login details during the potential scam call. But he didn't feel there was enough reliable information about or record of this call – and also wasn't persuaded it was likely her card could have been intercepted when posted to her.

The investigator also wasn't satisfied Ms H had accounted for a large credit into her account shortly before the disputed activity (which equated to most of the loss) which she said was money owed to her by a family member. He also wasn't satisfied with Ms H's explanation of why her online banking use changed during the period of the withdrawals. She had previously been accessing it regularly, but then didn't use it after 23 December 2023 until after the last withdrawal was made on 13 January 2024. Ms H said this was due to being busy with family over the holiday period.

Ms H has appealed the investigator's outcome. She says a new device was added to her account and used to view her PIN and order a new card, which was sent to a mailbox outside her property, and a fraudster used it to make the withdrawals. She also says she didn't keep years of phone records and messages as she didn't know she would fall victim to fraud. And that Halifax should obtain CCTV footage from the ATMs where money was withdrawn.

**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.

I appreciate this will be disappointing for Ms H. But, for the following reasons, I've decided not to uphold it.

Here, it's clear there is a disagreement between Halifax and Ms H about what happened. The basis on which I have made my decision is the balance of probabilities. So, where information is unclear or contradictory, I've decided what's more likely to have happened based on what is available.

Ms H has told us she received a call from someone pretending to be from Halifax in December 2023 and was tricked into sharing her login details. That could account for how an unauthorised person could have added a new device to the account to view her PIN and order a new card. However, when reporting the dispute to Halifax – when her memory will have been most fresh, so is what I place most weight on – she told it she hadn't shared her login details.

If Ms H didn't give out her login details during the call, it's unclear how a fraudster could have accessed her account. Additionally, Ms H hasn't been able to provide a record, or many firm details, about the scam call. I do appreciate the difficulty in providing this information, especially now so long after the event. But this is also something Halifax asked for when she first reported her dispute – which would have been a month or so after the call.

I'm also conscious Halifax's audit information, which I consider reliable, shows Ms H was sent a text notifying her that a new card had been ordered. I do consider it unusual that she would therefore have missed or not received this text, as she has told us. (Halifax says this also prompted an automated confirmation call, but I consider it less clear which device this went to and so I haven't relied on this.)

It appears messages were also sent by online banking – which Ms H accessed after the new device and card were set up. I'm persuaded she was also sent a further message on 25 December 2023 about her phone number being changed, prompting her to get it touch if this wasn't her. But she didn't do so until 13 January 2024.

A new card was posted to Ms H's home address. She says she had been experiencing issues with receiving post but again has no record of this (such as a record of reporting any problems or details any other post that went missing). I appreciate her post box appears to have been outside her home – but it still isn't clear how this could have been accessed by someone other than Ms H without her realising. So, I do question how a fraudster could have intercepted her card to use it.

Furthermore, if the new device was set up by a fraudster, they would already have access to Ms H's online banking – seemingly including her other Halifax accounts, as funds were transferred in from them to fund some of the withdrawals. It therefore does strike me as unusual that a fraudster wouldn't use this access to more quickly and remotely make payments – rather than ordering a card, which they would need to intercept, and then making a series of excursions to an ATM used previously on the account to drain funds over a period of over two weeks.

There are some further circumstantial factors that I consider relevant here. Looking further at the account use, there was a substantially higher balance than normal. This was largely down to a credit of almost £5,500 paid into the account a few days before the new device was added, originating from a business account and paid in (originally to another account held by Ms H) with the reference "Vauxhall Corsa".

Ms H says this was money owed to her by a family member who held the business account. But she hasn't been able to provide any records, such as contemporaneous messages, to support what this related to (or, indeed, why it was being paid from a limited company account).

I do also agree with the investigator that there is a distinct change in how the account was used by Ms H during the period of the dispute. I do appreciate this occurred over a holiday period. But there was a switch from her checking her account very regularly, to then not accessing it at all for around three weeks. It also appears no further transactions were attempted after the fraud was reported despite some funds remaining in the account.

In saying all of this, I do accept that I can't be sure what happened here and I don't consider it impossible the withdrawals were done by an unauthorised person. However, as mentioned above, what I'm considering is what is more likely to have happened. Weighing up all the factors here, I don't think Ms H's explanation for how an unauthorised person could have made these transactions is the more likely one.

While Ms H has suggested it should be on Halifax to obtain CCTV evidence, I agree with the investigator that this information isn't necessary for us to reach a fair decision here. CCTV footage won't be available at this point. Nor do I think it would be decisive; even if it showed someone else making the payments, that wouldn't show whether Ms H may have shared her card. I also haven't seen records supporting Ms H's assertion that the police told her Halifax should be the party to request this.

Overall, I consider it fair for Halifax to treat these payments as authorised and to therefore hold Ms H liable – given its obligations under the Payment Services Regulations 2017 to process unauthorised payment instructions without undue delay.

**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 Ms H to accept or reject my decision before 5 February 2026.

Rachel Loughlin
**Ombudsman**