DRN-6276359

The complaint

Mrs S complains that transactions she didn't make or authorise debited her credit card account held with Bank of Scotland plc.

What happened

Mrs S says that in November 2024 she was out shopping and placed her bag on the floor. Her bag was stolen and this contained her purse and bank cards – including her Bank of Scotland credit card. Her phone was also in her bag which contained personal information and security credentials. Mrs S has confirmed her phone was not password protected.

A number of transactions debited Mrs S' account which she says she didn't make or authorise.

Mrs S says she contacted Bank of Scotland immediately to report the theft and asked for a block to be placed on her account to stop further transactions, but this didn't happen. Bank of Scotland have said they didn't receive any contact from Mrs S until 27 December 2024. Bank of Scotland didn't uphold the complaint on the basis that the transactions appeared to be genuine.

Our investigator explained it was difficult to establish exactly what had happened in this case as Mrs S has been unable to confirm the exact date her bag was stolen. However, she didn't uphold the complaint for the following reasons:

- There was no record that Bank of Scotland were notified Mrs S card was stolen prior to 27 December 2024, despite the theft occurring around November time.
- Although Mrs S said she contacted Bank of Scotland prior to this by email, she couldn't provide a copy of this to support her testimony.
- Mrs S had reported her debit card (also held with Bank of Scotland) as stolen on 17 November 2024 through her online banking, but she didn't take any action in relation to her credit card.
- Mrs S previously had fraud on her account which may have been enabled because her phone wasn't passcode or biometrically protected. So Mrs S ought to have been aware of the risks involved in continuing not to have her phone protected and the risks of storing her personal details.
- The account terms and conditions require Mrs S to keep her card, details and device safe and to contact Bank of Scotland as soon as possible if the card is lost or stolen.
- The online banking records suggest Mrs S was able to login via her usual device using the same IP address from 13- 24 November and the passcode was used. Mrs S habitually entered her password once incorrectly and then correctly on the second attempt, this pattern of behaviour continued. This suggests Mrs S had possession of her device which brings into question Mrs S' version of events.
- Even when a new device was added on 24 November, it would seem the same IP address was used.

- The fraud wasn't typical behaviour as the funds in the account weren't maximised straight away.
- There were refunds into the account from some of the merchants which would suggest whoever had the card had returned some of the items purchased – which seems highly unusual.

Mrs S didn't agree although didn't put forward any additional points or evidence to support her testimony.

As Mrs S didn't agree, the complaint was passed to me to decide. I issued a provisional decision. I've set out my findings again below and they form part of this decision.

Provisional findings

I've considered all the available evidence and arguments to decide what's fair and reasonable in the circumstances of this complaint.

The relevant regulations here – the Payment Services Regulations 2017 – say that generally a consumer won't be held liable for any transactions made on their account that they didn't authorise, except in limited circumstances. In this case the most important question I need to answer is whether I think it's more likely than not Mrs S, or someone acting on her behalf, authorised the transactions.

Authorisation

I am in agreement with the investigator that it's hard to determine exactly what happened when Mrs S herself isn't clear on the timeline of events.

I understand Mrs S has memory issues so cannot recall the specific date of the theft. However, Mrs S has always said it was November 2024 when her bag was stolen and this contained her purse including her credit card and debit card held with Bank of Scotland. I should also explain this complaint only focuses on the credit card.

Mrs S' bag also contained a card relating to another bank (which I'll call "M"). The records relating to the case with M show that Mrs S thought the theft occurred around 14 November 2024, although she couldn't be certain. For the purposes of this complaint, I have worked on the basis the theft occurred around this time.

Mrs S' has consistently told us and Bank of Scotland that her phone wasn't protected and her notes contained sensitive information. It seems that this may have included her PIN for her credit card and the passcode for her online banking (amongst other things). Our investigator proceeded on the basis that this information was on her phone and Mrs S hasn't disputed this. Our service did contact Mrs S twice to double check but we didn't receive a response. As such I have proceeded on the basis this information was available on Mrs S' phone.

Bank of Scotland have said the transactions that took place were a mixture of contactless, chip and PIN and online. As Mrs S had stored her PIN on her mobile device which wasn't protected, it's feasible that whoever had Mrs S' phone also had access to this sensitive information to enable the transactions to take place.

Bank of Scotland have also said the online transactions were verified by a text message sent to the number held for Mrs S. It's feasible that whoever had Mrs S' phone was able to authorise these transactions.

Having looked at Mrs S' online banking records it seems that the log in used her same device and the same IP address from 13 November 2024 to the 24 November 2024. The records also indicate Mrs S wasn't able to log on straight away on the first attempt but was successful afterwards. The records show this continued to be the case over this period.

But I wouldn't expect to see this from a fraudster using the details found on Mrs S' phone. I say this because even if a fraudster got the details incorrect on the first attempt, I'd expect further attempts to be successful on the first go. I also find this unusual as it seems the details to access Mrs S' online banking were stored on her unprotected phone.

It's also unlikely that a third party was aware this is how Mrs S would usually access her online banking and would go to the effort of continuing this behaviour. So this does suggest it may have been Mrs S accessing her online banking. This would call into question Mrs S' testimony including her position that her phone was taken.

The records relating to Mrs S online banking also show on 24 November 2024 a new device was added and biometrics updated. The login on 25 November 2024 shows the same IP address being used as the IP address prior to this date, showing the phone was in the same location. So again, this calls into question Mrs S' testimony as I don't think it's likely the online banking was accessed at the same IP address by an unauthorised third party.

Having looked at Mrs S' statements, I can see that some of the disputed transactions were refunded by the merchants suggesting goods had been returned. I find it highly unlikely that a fraudster would go to the effort of seeking a refund from the merchant as they would have nothing to gain from doing so.

Mrs S has told us she reported the theft to the police but has been unable to provide a copy of the police report. So this does further call into question the reliability of Mrs S' testimony as she doesn't seem to be able to substantiate what she's told us.

I appreciate Mrs S will be upset by this as she's concerned about paying back what she owes. She also feels that Bank of Scotland haven't helped especially as M have refunded her. But based on all the evidence that's been provided, I'm not satisfied it wasn't Mrs S (or someone else authorised on her behalf) that carried out these transactions so I do not think Bank of Scotland has done anything wrong in holding her liable.

The records provided by Bank of Scotland show Mrs S cancelled her debit card on 17 November using her online banking. I would have expected Mrs S to have also cancelled her credit card at the same time, in particular as she'd have been aware of that the sensitive information contained on her phone was also in relation to this account. But again Mrs S has failed to take such steps.

The account terms and conditions also require Mrs S to contact the bank as soon as possible if fraud has occurred.

Mrs S said that she contacted Bank of Scotland immediately after the fraud had taken place by email. Our service asked for a copy of this email which Mrs S initially said she had, but unfortunately, it still hasn't been sent to us.

Having looked at Bank of Scotland's records, I can't see that they received any contact from Mrs S regarding the theft of her credit card and they weren't aware of the fraud until 27 December 2024. So given that the fraud occurred around 14 November 2024, I can't agree that Mrs S contacted the bank as soon as possible.

Mrs S did say she had contacted Bank of Scotland by phone on 11 December 2024. But even if I were to accept Mrs S reported the fraud on this date, I can't agree this was soon after the fraud had taken place – as it was approximately a month later.

So taking everything into account I don't think Mrs S has adhered to her terms and conditions.

Looking at the complaint overall, I do not think Bank of Scotland have acted unfairly in holding Mrs S responsible for the transactions in question, as I find it most likely that they were authorised in some way by Mrs S herself.

My provisional decision

My provisional decision is that I do not uphold this complaint.

Neither Mrs S nor Bank of Scotland replied by the deadline we set.

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.

In the absence of any new information or evidence presented to me I have no reason to depart from the findings as set out in my provisional decision.

My final decision

For the reasons I've explained above, I don't uphold this complaint.

Under the rules of the Financial Ombudsman Service, I'm required to ask Mrs S to accept or reject my decision before 6 May 2026.

Marie Camenzuli
Ombudsman