

The complaint

Mr M complains that Bank of Scotland plc trading as Halifax ("Halifax") failed to refund transactions he didn't recognise.

What happened

What Mr M says

Mr M explained that during a night out, he became intoxicated and early in the morning was trying to get a taxi home. He recollects having difficulty ordering one and eventually got into a car he thought was a taxi.

Mr M's recollection of the events that followed are a little unclear due to his state of intoxication, but he remembers being shouted at by the driver. He's said the next occasion he remembers is being in the road and awake about 4-5 hours after getting into the "cab".

Mr M's phone, jacket, watch, and drivers licence were missing, but his wallet and debit card were still present. Mr M was able to get home after a passer-by gave him a lift and he later reported the theft of his items to the police and notified the phone company about the loss of his phone. It wasn't until later that day when Mr M became aware that his Halifax account had a number of transactions present that he didn't recognise, including cash withdrawals from an Automated Teller Machine (ATM) and bank transfers made using his mobile banking facility.

Mr M spoke with Halifax the evening of the incident and explained some of what happened. Mr M confirmed that he hadn't told anyone else the PIN number or given permission for the use of his account by anyone else. Mr M believed that his account had been used by third parties without his permission whilst he was incapacitated, and they'd used his fingerprint and control of his phone to carry these payments out, including a PIN reminder to make the ATM withdrawals.

Mr M and Halifax spoke on a number of occasions about the incident, but Halifax declined to make any refund, believing the evidence of the transactions indicated Mr M himself was responsible. Mr M disagreed and made a complaint, including about the way that Halifax dealt with him. Halifax again looked into the circumstances and believed they'd dealt with Mr M appropriately and there was no evidence of a third party being involved, so offered no refunds. Mr M then brought his complaint to the Financial Ombudsman Service for an independent review.

What Halifax say

Halifax received Mr M's request for a refund after he notified them of the issues with his account following a night out. Halifax's systems identified that the payments made from the account were done using biometric authentication (Mr M's fingerprint), including a request on the same morning to view the personal identification number (PIN) through the mobile banking app.

Based on this information and Halifax's view that Mr M's version of events was inconsistent, they declined to refund him and turned down his complaint.

The investigation so far

Both parties were asked to supply information about the complaint and Mr M wrote to our service with his best recollection of what happened to him the morning of the disputed transactions – the summary of which is set out above. Mr M believed that Halifax had misinterpreted his situation.

Halifax provided audit data concerning the use of the card for the ATM withdrawals and the use of Mr M's mobile banking app on his phone to transfer funds between his accounts and set up the outgoing payments to a new payee.

The data showed that:

- The mobile app was logged into using biometrics (fingerprint).
- A request was made to view the PIN (which wasn't considered unusual by Halifax).
- Funds were transferred from a savings account into the current account.
- A new payee was set up and authorised using the biometric data and confirmed through additional steps using the app after a message was sent to it.
- One ATM withdrawal and one large bank transfer were blocked by Halifax's systems.
-

Halifax commented that Mr M's version of events was inconsistent and coupled with a lack of explanation how his account could have been compromised, declined him a refund. They also remarked that Mr M hadn't called them for some hours following the realisation that he'd lost funds.

After reviewing the evidence, the investigator assigned to assess Mr M's complaint thought that:

- It was reasonable for Halifax to process the various requests for funds because they used the appropriate account procedures including One Time Passcodes (OTPs) and Mr M's biometrics.
- IP address data matches with earlier use by Mr M.
- Mr M's version of events is inconsistent and can't be relied upon.
- Passwords for the phone and the banking app were different meaning two sets of data needed to be obtained in order to bypass it.
- There was a PIN reminder request, but this wasn't out of the ordinary.
- Mr M retained possession of his bank card.

Mr M's complaint wasn't upheld by the investigator. Mr M disagreed with the investigator's outcome and said he was incapacitated so couldn't have agreed to these transactions at the time. He also pointed out that whilst there were different passcodes for his phone and banking app, they were both also accessible via biometric means.

Some discussion was held regarding the timings of certain account transfers/withdrawals and the use of the OTP's. Mr M continued to argue that he wasn't responsible for these transactions and asked for a further review of his complaint, which has now been passed to me for a decision.

As part of my own investigation, enquiries were made with the investigating officer concerning the allegation made by Mr M. The police have responded and concluded that whilst their investigation is ongoing, they believe Mr M was the victim of a crime that morning

after he left the club whilst intoxicated.

I issued my provisional findings on the merits of Mr M's complaint on 17 November 2023. In my provisional findings, I explained why I intended to uphold Mr M's complaint and offered both sides the opportunity to submit further evidence or arguments in response. An extract of that decision is set out below and forms part of this final decision:

What I've provisionally 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.

The relevant law surrounding authorisations are the Payment Service Regulations 2017. The basic position is that Halifax can hold Mr M liable for the disputed payments if the evidence suggests that it's more likely than not that he made them or authorised them.

Halifax can only refuse to refund unauthorised payments if it can prove Mr M authorised the transactions, but Halifax cannot say that the use of the card and PIN or the use of internet banking conclusively proves that the payments were authorised.

Unless Halifax can show that consent has been given, it has no authority to make the payment or to debit Mr M's account and any such transaction must be regarded as unauthorised. To start with, I've seen the bank's technical evidence for the disputed transactions. It shows that the transactions were authenticated using the payment tools issued to Mr M. I'll now need to consider the information provided by both parties to determine whether there's sufficient evidence to hold Mr M responsible for the disputed transactions or not.

There's no particular argument here that Mr M's genuine debit card was used to withdraw funds from an ATM using his PIN, also that Mr M's mobile banking app loaded on his phone was used to make internal transfers and bank transfers to another account, authenticated using the biometric function set up on his account (and phone). The evidence also shows that a PIN reminder was viewed at the time of the incident reported by Mr M.

The crux of this complaint is that Mr M denies making these transactions and believes other parties were responsible after he was incapacitated. Halifax don't believe there's an explanation for how the account was compromised and think that Mr M's version of what happened was inconsistent.

So, I need to decide what likely happened, even though I wasn't present and Mr M's memory of the event is patchy. If Mr M made the payments himself, then he would be liable for them, on the other hand, if Mr M was incapacitated and couldn't make the transactions himself, then he couldn't be held liable, and Halifax would have to refund them because they would be unauthorised.

The circumstances detailed by Mr M show that he was incapacitated – he's also said he was, for some period, unconscious. Whilst there's no medical report to show what caused this condition in Mr M, I don't doubt his explanation. It could have been something he ingested unknowingly or just over consumption of alcohol.

I understand the stance taken by Halifax on this complaint (the audit data points to Mr M being responsible), but I don't put the same reliance on the inconsistencies as they do. Considering Mr M was, at the very least, heavily intoxicated, I'm not surprised that other details have emerged or evolved as the various conversations were held with Halifax. I don't think it's unreasonable for someone's recall under similar conditions to change somewhat.

The period of incapacitation raises a difficulty when trying to understand what went on for those hours Mr M can't recall. We know that his phone was used to access his banking app, obtain a PIN reminder for his phone, transfer funds between accounts and set up a new payee and make payments to them. I'd argue that completing the transfers to a new payee (who Mr M says he doesn't know and wouldn't have agreed to send funds to) at that time in the morning when numerous ATM withdrawals have been made is untypical behaviour.

Halifax have argued there's no evidence of a compromise of Mr M's account (because it used the appropriate means to withdraw funds (account card & PIN) and access to the banking app authorised by biometrics and OTPs. But, if Mr M's version of events is to be believed, the use of his fingerprint biometrics seems a plausible explanation for how both his phone and the banking app were opened. Once control of the phone was obtained, the response to any OTPs would also be realistically possible.

I've also looked at other factors surrounding this complaint, including the report to the police about what happened. Mr M seems to have told them generally the same version of events provided to our service. Having obtained a response from the investigating officer, it seems the report made by Mr M is credible and that he's considered a victim of some form of criminal activity early that morning, although their investigation is ongoing.

My provisional decision

Taking all the evidence into account, my current thoughts are that Mr M himself didn't complete the necessary steps to authorise the payments himself, and that others, without his permission did so. I'm currently intending to uphold Mr M's complaint and require Halifax to refund all the disputed transactions.

I invited Mr M and Halifax to give me any more evidence and information they wanted me to consider before issuing my final decision. Both parties accepted my provisional decision and Halifax helpfully set out the redress they intend to pay to Mr M, being £2,000 for the bank transfer, £450 in respect of ATM withdrawals and to include 8% simple interest from the date of the loss to the date of settlement.

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, and as both parties accepted my provisional decision, I see no reason to reach a different conclusion. So, this final decision confirms the findings set out in my provisional decision.

I'd like to thank to both parties for responding as quickly as possible to the provisional decision.

Putting things right

Halifax to pay Mr M £2,450 including simple interest at 8% from the date of loss to the date of settlement.

My final decision

My final decision is that I uphold this complaint against Bank of Scotland plc trading as Halifax and they're required to settle it as outlined above.

If Halifax considers that it is required by HM Revenue & Customs to withhold income tax from that interest, it should tell Mr M how much it's taken off. It should also give Mr M a tax deduction certificate if he asks for one, so he can reclaim the tax from HM Revenue & Customs if appropriate.

Under the rules of the Financial Ombudsman Service, I'm required to ask Mr M to accept or reject my decision before 4 January 2024.

David Perry
Ombudsman