DRN-4739030

The complaint

Ms C complains that Bank of Scotland plc trading as Halifax (Halifax) won't refund two transactions totalling £1,189 which she says she didn't authorise.

What happened

The background to the complaint is well known to both parties, so I'll provide only a brief summary here.

- Halifax texted Ms C to contact them about a new payee that was added to her current account if she hadn't added them.
- Ms C then phoned Halifax but wasn't willing to continue with the call and enter her account number.
- Ms C then logged into her account and noticed that £754 and £435 had left her account. She says she didn't authorise these transactions.
- Ms C says that she subsequently learnt that someone else had registered for the mobile app one week before the transactions took place. She believes that this was how the transactions were made.
- Halifax confirmed the payments were made through the mobile banking app and that the device used to make payments had been registered a week prior to the transactions. They explained that this was done after completing an automated phone call. This call went to the mobile number Halifax has registered for Ms C.
- Halifax said that they sent Ms C a text a week prior to these transactions informing her that she had registered for the mobile app. However, they said they didn't hear from her until after the transactions took place (a week later).
- Halifax believes that Ms C authorised these transactions.

Following the provisional decision additional information has been provided which I have carefully reviewed.

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.

While I might not comment on everything (only what I consider key) this is not meant as a discourtesy to either party – it reflects my role resolving disputes with minimum formality. I'd like to assure both parties I've considered everything they have sent including the additional information provided following my provisional decision.

Having done so, I'm intending to reach the same conclusions as set out in my provisional decision for materially the same reasons. I'll explain why.

Before I set out my thoughts, I want to acknowledge that I have summarised this complaint briefly and in less detail than has been provided. I've focused on what I think is the heart of the matter. While I may not comment on every point raised, I have considered it. I'm satisfied that I don't need to comment on every individual point or argument to be able to reach what I

think is the right outcome. Our rules allow me to do this and reflect the fact that we are an informal service and a free alternative for consumers to the courts.

Generally speaking, Halifax is required to refund any unauthorised payments made from Ms C's account, and Ms C should only be responsible for transactions made on the account that she has authorised. Those rules are set out in The Payment Service Regulations 2017. Ms C said she didn't carry out the transactions in dispute. So, I have to decide whether or not I think she did authorise the transactions.

Mobile banking app

It's not disputed that the transactions were completed through the mobile banking app. Ms C says that she didn't apply for the mobile app and therefore didn't authorise the transactions.

Ms C has provided screenshots which she says shows that she didn't download the mobile banking app. I've carefully reviewed these screenshots. However, it is not evident that the screenshots are from Ms C 's device, nor is there confirmation that this was the only device she was using at the time the app was installed. The screenshots are undated, and it is also unclear whether they would display apps that have since been uninstalled. Therefore, the screenshots are not enough for me to conclude, on the balance of probabilities that C did not install the mobile banking app.

Ms C indicated a fraudster could easily bypass security to set up a mobile banking app, and provided screenshots of her friend going through the set up process to demonstrate this. She believes this shows the app can be set up with limited information, and should be taken into consideration when determining who had registered for the app.

I've carefully reviewed these screenshots, and they refer to registering for online banking, not specifically setting up a mobile banking app. (Ms C says she is providing this as she hasn't registered for the mobile banking app). Looking over these screenshots I can see that registering for online banking also requires a password to be given and it's unclear how a third party would have had access to the password. These screenshots are also not from the time the mobile app was set up and may be a different process from the time the disputed transactions took place. So I can't say that these screenshots persuade me that somebody else could have easily have set up a mobile banking app on Ms C's account.

I've also asked Halifax for a bit more information around this to see what would have been needed when the app was set up on 18 October 2023. The screenshots Halifax provided show the steps that needed to be completed specifically around registering a device, which entails entering memorable information and submitting a code which Halifax would have provided by calling Ms C using the number Halifax had for Ms C. Halifax has had the same contact number for Ms C since 10 March 2023 (and I've noted it is the same number our service has for her). So I'm persuaded Halifax would have contacted her on this number.

Ms C has said her password for online banking was the same as an entertainment account she had linked to her phone provider account. She further notes that Halifax confirmed her username in an email it sent to her on 13 October 2010 and it's possible her email account could have been compromised. While I appreciate Ms C's point, I have to base my decision on what on balance is most likely to have occurred, and there isn't enough here for me to say her phone and phone account were compromised allowing a third-party access to her security details. In addition, looking over Halifax's website it's clear the memorable information and online password are two distinct pieces of security credentials, and I can't see how it's likely Ms C's memorable information was also compromised.

Based on the evidence I've seen I think it's fair to say that a mobile device had to be registered before a mobile banking app could be set up. This involved submitting a code that Halifax provide by calling, and also by entering memorable information. Ms C says she couldn't have taken a call at that time as she was engaged in completing the transaction. While I understand Ms C's point the fact that she was making a payment does not, in itself mean she was unable to receive a call and note down a verification code. And I haven't been provided with any information to show how anyone, but Ms C, would have had access to the code or could have received the phone call on 18 October 2023.

Ms C also provided a screenshot showing that she received an email titled "Halifax – Welcome to online banking" on 18 October at around 18.07 which she says she received shortly after she logged off after making a legitimate payment to her sister (and there is an entry entitled "Halifax – Logged Off" with a time stamp of 18.01). However, the timing of the email isn't sufficient for me to say Ms C account was compromised.

Ms C's itemised phone bill doesn't show any calls from Halifax on 18 October. This could suggest that it wasn't her who Halifax called on 18 October. However, I don't think her phone bills prove she didn't receive a call from Halifax for the following reasons:

- It's not uncommon for phone bills to omit incoming calls.
- Ms C's mobile network provider's website says an itemised bill will show who "you've called and messaged" but doesn't say incoming calls or texts are displayed.
- Ms C provided an email from her mobile network provider dated 18 April 2024 stating they only provide records of outgoing calls and texts, apart from in certain circumstances where a court order is involved, as these are considered third party disclosure.
- Halifax's internal notes show that a successful call was made to Ms C on 18 October 2023 when the device was set up (at around 6.00pm).

I appreciate that Ms C says a manager at her phone provider branch assured her that the bill she was given contained all calls received. I've carefully weighed this up alongside the email and details mentioned above. Having don so I'm not persuaded there's enough for me to say the itemised phone bill showed the incoming calls Ms C received.

I acknowledge that Ms C says she didn't receive a call or text. However after carefully reviewing the information given from each side, I'm persuaded that the phone call did occur. I also haven't been provided with any information to show how someone else other than Ms C would have had access to the memorable information needed to complete the mobile phone registration. I appreciate that Ms C says she was going to provide technical evidence to show this happened, however based on what I've seen I can't say that this likely occurred.

In addition, after the app was set up Halifax said it sent a text to Ms C confirming that this had been done. Ms C said that she didn't receive the text. Halifax has provided a copy of its internal notes showing that a text was sent and that it said "you registered for Mobile Banking on 18/10 at 17:58:30. If this WASN'T you call us". The text then provides Halifax's contact details. I haven't been provided with anything to show that there were any issues with Ms C receiving the text, or that she had any concerns about her phone at this time. Just as I'm persuaded that the phone call did occur, the bank's supporting evidence persuades me that it sent Ms C a text and that on balance this was received to Ms C's registered mobile telephone number.

Transactions 25 October

Ms C confirmed she did receive texts from Halifax one week later (25 October) informing her that a new recipient had been added to her account. Halifax has provided a copy of the text

sent which reads “you set up a new recipient on 25/10 at 19:06:06 from account ending XXXX. If this was not you please call” followed again by Halifax’s contact details. Ms C said she didn’t immediately respond as she was commuting home, she also didn’t continue a call with Halifax as she didn’t want to type in her account details into her phone.

Once Ms C says she became aware of the transactions, she said that she searched online the name of the person who she believes debited the funds from her account – the name that was showing on her statement. Ms C said that according to her search, this person worked at the same mobile network provider Ms C uses. She said that they have access to her “full name, address, date of birth, secret password on the account, my account number and sort code and email address”. She believes that this is enough for somebody to gain access to her account.

Based on what I’ve seen I’m not persuaded this information would have been enough to set up mobile banking, as they would also have needed to have known Ms C’s memorable information, and I haven’t been provided with any information to show the mobile network provider had access to this. I also haven’t been provided with any information to show how somebody else would have had access to the code sent to Ms C’s mobile phone when she set up the mobile banking app. So while I appreciate Ms C’s comments, there isn’t enough here for me to say an employee at Ms C’s mobile network provider used the information Ms C provided to them to set up mobile banking in order to take funds from her account without her consent.

I’ve also noted that it is unusual that the mobile banking app was set up on 18 October and funds weren’t taken from the account through the app until 25 October. The statements given also show the amount in the account stayed roughly the same during this time.

To determine whether Ms C likely authorised the two disputed transactions, I need to firstly be satisfied that Ms C authenticated the transactions. The transactions were authenticated using the mobile banking app. Based on the manner in which the mobile app was set up, using Ms C’s mobile number and memorable information there isn’t enough for me to say Ms C didn’t set up the app and subsequently approve the transactions. I haven’t been provided with any information to show how somebody else had access to her phone when the mobile app was set up, or a week later when the funds were taken from her account. And while I appreciate Ms C’s point that an employee at her mobile phone provider would have access to a lot of her personal information – it’s unclear how they would also have had access to the memorable information, or code Halifax provided which was needed to register the mobile device before the mobile app is added.

In this case, based on the evidence provided, I can’t see any plausible explanation for how this would likely have happened and how the transactions could have been completed without Ms C authenticating and consenting to the transactions.

Customer service

Ms C has also said that she wants Halifax to compensate her for the stress, anxiety and hardship she incurred and the constant chasing she had to do to obtain updates. When looking into awards for distress and inconvenience my role is to focus on the actions of Halifax and the impact those actions had on Ms C. My role isn’t to punish or regulate Halifax.

I want to firstly acknowledge that Ms C has spent a lot of time and effort in bringing this complaint, and that raising a complaint will always to some extent involve some level of inconvenience. She has also contacted numerous third parties, however within this complaint I’m limited to only commenting on the actions of Halifax.

The transactions occurred on 25 October and Ms C complained about them to Halifax that day. A final response was issued on 9 November, and Ms C briefly spoke to an adviser that day who told her the outcome of her complaint. Halifax has also provided a copy of the call recording that took place between their adviser and Ms C dated 10 November 2023 – where the outcome of the complaint was discussed and Ms C confirmed that she would be bringing this complaint to our service, which is within the 15 working days Halifax is allowed to respond, according to the regulations. So I don't think there has been an unnecessary delay here. I appreciate that Ms C told us that she repeatedly chased Halifax for a response, by phone and by visiting the branch during her lunch hour and after work. And is frustrated that it appears that a complaints manager was only allocated once she called in and this was escalated. It's clear that Ms C spent a lot of time and effort in trying to get this resolved. However, considering the overall circumstances, I don't think there has been an unnecessary delay in Halifax investigating her complaint as they provided her with a response within 15 working days.

I appreciate that there appears to be a delay in Ms C receiving Halifax's written response to her complaint, dated 9 November 2023. Ms C acknowledged that she received the final response by email on 16 November 2023 and finally by post on 27 November 2023. Given the short length of time involved here and the fact Ms C already knew what Halifax's position was, I don't think Ms C was materially impacted, so, I'm not asking Halifax to compensate her for this delay. Though I do want to acknowledge the time and effort Ms C has spent in bringing this complaint.

My final decision

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

Under the rules of the Financial Ombudsman Service, I'm required to ask Miss C to accept or reject my decision before 13 June 2025.

Sureeni Weerasinghe
Ombudsman