

## The complaint

Mr F and Ms W complain that HSBC UK Bank Plc are holding them liable for what they say are unauthorised transactions made on their account.

Whilst the account in question is a joint account, for ease of reading and as he's done all the correspondence on the complaint, I'll mostly just refer to Mr F where I mean both him and Ms W.

## What happened

The detailed background to this complaint is well known to both parties. So, I'll only provide an overview of some of the key events here.

Mr F says that on the evening of 4 June 2022 he was out with friends. Late in the evening he realised his phone was lost or stolen. In the early hours of 5 June 2022, there were multiple unsuccessful attempts to log in to Mr F's HSBC mobile banking app, resulting in the app being locked.

Mr F's app for an account he held with another business 'R' was accessed. And from there debit card 'top-ups' were made to credit the account with R, using the credentials from Mr F's HSBC debit card. There were also unsuccessful attempts to move money in this way. Ultimately a total of £4,510 was moved from the HSBC account to the account with R via this method.

Also overnight a £10,000 loan with a lender I'll refer to as 'L' was paid into Mr F's HSBC account. And some of the funds moved to R came from this loan. Once the funds were in the account with R, card spending took place for approximately £4,500 which involved goods being ordered online before being collected in a store.

In summary Mr F says he knows nothing about any of this activity with either HSBC, R or L. He says he's been a victim and didn't apply for the lending or authorise any of the payments. He says when he discovered all this he reported it to each business. He also returned to L over £5,000 of the loan funds that remained in his HSBC account. Mr F complained to all three businesses.

L said they couldn't do more at the time as they were awaiting a copy of HSBC's fraud investigation. HSBC essentially said that Mr F should take this matter up with R, as the funds were all transferred into his own account with them and they deemed R to be the point of loss. R similarly didn't uphold Mr F's complaint.

All three complaints were referred to our service. The complaint about R has already been decided by one of my Ombudsman colleagues. A final decision was issued in December 2022 which didn't uphold the complaint. The Ombudsman said *"I consider it reasonable that [R] held Mr F responsible for the payments as being authorised."*

One of our Investigators considered the complaints about L and HSBC. They didn't uphold

either. For the HSBC complaint the Investigator thought it more likely than not that Mr F had consented to the transactions from his account. Mr F strongly disagreed and asked for an Ombudsman to review his complaint.

In November 2023 I issued a provisional decision in which I said:

*"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, I'm intending to reach the same overall outcome as our Investigator. But as there are some minor differences in my reasoning, I'm issuing this provisional decision to give everyone a further opportunity to comment before finalising my decision.*

*I'm aware of Mr F's linked complaint about L. But this decision only relates to whether HSBC have treated Mr F fairly and reasonably in all the circumstances.*

*Mr F's strength of feeling about this complaint is clear. And accordingly he's made some detailed submissions. I've read and considered all Mr F has sent in, but I won't be responding in similar detail. This isn't intended as a discourtesy and is just a reflection of the informal nature of our service.*

*The Payment Services Regulations 2017 (PSRs) are a key consideration to this complaint. Generally speaking customers will only usually be liable for payments made from their account if they 'authorised' them. Authorisation in this context requires both authentication (through the agreed process for making a payment) and consent. So it isn't enough that the payments were correctly authenticated, if Mr F hadn't consented to them, then he wouldn't generally be responsible for them.*

*I'm satisfied that each of the payments that left Mr F's HSBC account were correctly authenticated using the details of his debit card that was presumably saved on R's platform. The card activity report from HSBC that I've seen confirms this and it also indicates that further authentication was completed via text messages being sent at the time. But I still need to consider whether Mr F consented to these payments or had no involvement as he claims.*

*The payments concerned were instructed from within R's app. To be able to do this, someone would have needed to have had Mr F's physical phone. They most likely would have needed to have bypassed the phone's own security (which Mr F says was fingerprint and passcode protected) and to have entered a PIN code to access R's app.*

*Mr F's testimony is that he doesn't know exactly how his phone was lost / stolen. He has suggested that he must have been pick-pocketed on the night out in question and that this could have been done soon after he'd put his unlocked phone in his pocket, prior to the phone locking itself again. He has also said that his emails within his phone weren't password protected and that they would have included a great deal of personal information about him, as he'd relatively recently moved house and documents relating to this would have been present. Mr F also said that the PIN for R's app was something that could be guessed as it was based upon some of his personal information.*

*None of the activity involved could have taken place without someone having access to Mr F's phone. Mr F says he didn't have the physical phone as it was lost / stolen. But as I've mentioned above, more than the physical phone was required to instruct the payments from his HSBC account.*

*Obviously I wasn't present with Mr F's phone when these payments took place. So I have to*

*make my findings on the balance of probability. That being, what I think is most likely to have happened, considering all the available evidence. The version of events Mr F has suggested to account for the compromise of his phone isn't impossible. I appreciate that fraudsters can be sophisticated and opportunistic as Mr F has said. I also appreciate the lengths Mr F has gone to in pursuing his complaint, which includes reporting matters to Action Fraud, writing to his MP and attempting to obtain CCTV from at least one of the bars he attended that evening.*

*The activity surrounding the HSBC mobile banking being locked does look suspicious and could be potentially indicative of third-party involvement. But there are a number of other possibilities which could explain such activity. These include that the log in details could have genuinely been forgotten or it could have been done to create doubt as to the nature of what went on. It also doesn't negate the possibility that it could have been a third party with Mr F's consent. So the fact that there were numerous failed attempts to log in, isn't in itself conclusive. And whilst I can't be sure why this happened, it does seem strange that a third party would have the loan paid into the HSBC account rather than the account with R (which they had access to) knowing it would be more difficult to disperse these funds.*

*Taking everything into account, I don't think the most likely explanation for what went on is that Mr F's security to his phone and app with R was compromised. This isn't a case where Mr F's phone was snatched from him whilst unlocked. If a device has biometric security and this is used (as Mr F says it was) then I think most people commonly use that functionality rather than regularly entering their passcode, negating the likelihood of it having been observed and used by a third party to access Mr F's phone. And I think most people habitually lock their phones when putting them away or into a pocket. But even if that wasn't the case, I think the chances of someone pick-pocketing Mr F at that exact moment, and then managing to keep the phone active long enough to change any auto-lock settings or otherwise bypassing the security, as well as correctly guessing the PIN for his app with R (even taking account of information that he says would have been available in his emails) whilst not impossible, on balance is unlikely. And given that finding, I don't think HSBC declining to refund the disputed transactions is unfair nor unreasonable. I think the most likely explanation, balancing all the evidence, is that Mr F had involvement in the payments he is disputing such that they can fairly be considered as authorised.*

*I appreciate much of Mr F's submissions have focussed on other issues. Such as whether HSBC ought to have intervened in the payments being made and whether his debit card should have been blocked when his mobile banking was locked. But as I'm supportive of HSBC's decision, none of Mr F's further points make a difference to the outcome of the complaint. So it follows, that because I think it's more likely than not that Mr F had involvement in the payments he is disputing, even if HSBC ought to have done more to question any of the payments to the account with R, I'm not persuaded that this would have made a difference.*

*Mr F has also focussed on the collection of the goods purchased from the payments made from his account with R. But as I've referenced above, this matter has already been decided by one of my colleagues who found that R had acted fairly when treating the payments as authorised. So, that isn't something I can comment on."*

HSBC responded to say they agreed with my provisional decision. Mr F provided some further comments which I'll address below.

## **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.

Much of Mr F's further responses primarily relate to his complaint about L. But where they are also relevant to his complaint about HSBC, I'll address them here.

Mr F's further submissions include that his phone was only passcode protected. He says there was no biometric security and he doesn't remember advising there was. My provisional decision referred to there being biometric security on the phone at the time. This was based on a call between Mr F and H on 6 June 2022. The context of the call was that Mr F was reporting that he didn't recognise the activity on his account. During that call the following exchange took place:

**HSBC:** *"May I know what type of phone did you lose sir? Was it an android or an iPhone?"*

**Mr F:** *"Android."*

**HSBC:** *"Was there a fingerprint scanner on that phone?"*

**Mr F:** *"There was yes and a passcode, so I'm not too sure how this has happened to be honest with you."*

I've shared this exchange with Mr F and he says his answer meant that his phone had the functionality to use a fingerprint scanner but it wasn't in use. He also clarified that it is not a two stage process and either a fingerprint (if in use) or a passcode can be used. I accept that its common, where a fingerprint scanner is in use, that the option usually exists to also use a passcode.

But in the context of the conversation Mr F was having with HSBC, I think it's more likely than not that Mr F meant that he did use biometric security on his phone. Had it been an option that wasn't in use, I think he would have stated this more clearly at the time. Particularly as the clear purpose of the question was to ask about the security features in use to help establish how someone might have accessed his phone. Ultimately, given my interpretation that I've explained above, I'm more persuaded by this phone call which took place around the time rather than what Mr F has said more recently. And given this finding, for the reasons previously explained, I'm still not persuaded there is a plausible explanation for how a third party could have accessed Mr F's phone which enabled all the further activity to take place.

Mr F has also speculated that rather than perhaps being pickpocketed, his phone could have been taken or lost whilst in a taxi returning him to his hotel at the end of the night. He also explained that he had been drinking on the day in question and thinks it's a possibility that the taxi driver could have taken advantage of the situation. However, Mr F's previous submissions to our service include an email in June 2023. In that email he said he'd been in the bar from which he later sought CCTV evidence and that he left *"around midnight where my stay at the bar was short, due to the realisation I didn't have my device."* But Mr F is now seeming to suggest that he did have his device when leaving the bar to get a taxi back to his hotel. So whilst I acknowledge Mr F has said he was drinking that day, the impact of him saying different things at different times makes it difficult for me to treat his testimony evidence as persuasive or reliable.

I accept that this is a balanced case and that I can't know with absolute certainty what happened. And also that the version of events that Mr F has described isn't impossible. But taking account of all the information and evidence provided, I don't think it was unfair nor unreasonable for HSBC not to treat the payments made from the account as unauthorised. And as such, I'm not going to direct that they need to do more to resolve this complaint.

**My final decision**

For the reasons outlined above, my final decision is that I don't uphold this complaint.

Under the rules of the Financial Ombudsman Service, I'm required to ask Mr F and Ms W to accept or reject my decision before 18 January 2024.

Richard Annandale  
**Ombudsman**