DRN-3959668

The complaint

Mr R complains that Barclays Bank UK PLC didn't refund him for several disputed transactions.

What happened

Around April last year, Mr R contacted Barclays because he didn't recognise some activity on his account. He says several direct debit indemnities were raised for payments he'd made – which included his phone bill, rent, car finance and university tuition fees.

Mr R says he didn't make these indemnity claims. Following the funds for these claims being returned to Mr R's account, several payments were made to third-party payees. Mr R says he didn't authorise these payments.

Barclays didn't agree to refund the disputed payments. The bank said it found no evidence of Mr R's account being compromised. It concluded that Mr R was liable for the payments because these were made using Mr R's mobile banking app. Mr R didn't agree and asked this service to review his complaint.

Mr R says:

- He believes his phone was hacked by a fraudster, who raised the indemnity claims and later paid out the funds for these claims into another account.
- He doesn't recognise the payees the funds were sent to.
- He didn't notice any unauthorised activity on his account until he received a letter regarding the indemnity claims. He says he expected funds in his account around the time, so he wasn't suspicious when the funds from the claims were credited to his account.
- He received several welcome messages on his mobile banking app, even though he hadn't reinstalled the app.
- He hasn't granted anyone access to his phone, his card has remained in his possession, and he hasn't shared his security information with anyone. Mr R says he did share some details with a prospective loan provider in February 2022, but decided to stop his application, as he was concerned about the level of information being requested.
- He's not been scammed, nor has he been asked to make a payment to someone.
- He's been financially impacted because he now owes money to the businesses the indemnity funds were claimed from.

Our investigator concluded that Barclays' decision was fair. Mr R doesn't agree and remains adamant that his phone was hacked. He also points to the indemnity claims, which he

believes were made over the phone – he thinks the calls should be listened to in order to establish that he didn't make them.

Because Mr R disagrees, his complaint has been passed to me to make a final decision.

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.

Barclays can generally only hold Mr R responsible for the disputed payments if the evidence suggests it was more likely than not that he authorised them. Based on what I've seen, I think it's most likely that Mr R, or someone he authorised, carried out these transactions – I'll explain why.

I'll start with the direct debit indemnity claims Mr R says he didn't raise. Mr R's testimony seems rational to me – it doesn't add up that he would initiate indemnity claims against payments he's made for essential components of his everyday life, such as his rent and university fees. Mr R says he was told by Barclays that the claims were raised over the phone, but this doesn't seem to be the case. Barclays most recently told us that the claims were made either via Mr R's mobile banking app or via its website. The bank's own notes indicate the claims were submitted online.

Although I can't say for certain how the claims were raised, it seems most likely to me that Mr R, or someone with his consent raised these claims. Barclays has sent information about the details that are needed to raise an indemnity claim. This includes Mr R's account and debit card details, address, contact number, email address and transaction details including the reference of the payment from his statement. Mr R hasn't pointed to anything that would suggest these details were compromised and I think it's unlikely that anyone other than Mr R would have access to all this information. So I'm not persuaded that someone other than Mr R raised these claims without his knowledge or consent.

Turning to the disputed payments made to third parties, whom Mr R says he doesn't know. Barclays has sent us Mr R's mobile banking log-in information – this shows me that it was Mr R's device that was used to log in and carry out the disputed payments. The bank's records show that each log in was made using Mr R's passcode; a detail that Mr R says hasn't been shared with anyone.

I can see that his mobile banking was logged in to using other devices around the time and new devices were also registered on his account. But the data shows that it was only Mr R's device that was used to make the actual payments and each new device registration seems to have been preceded by a log in from Mr R's own device – indicating to me that Mr R likely authorised these registrations.

Barclays says to register a new device, Mr R would've needed essential details about his account, including an SMS that would've been sent to his phone or his debit card alongside a PINsentry device. Given that no-one other than Mr R has access to his phone and his debit card, I think it's likely that Mr R carried out the registration of new devices around the time. This also provides a possible explanation for Mr R's submission that he received numerous welcome messages on his mobile banking app around the time – the dates of these messages seem to coincide with new device registrations a few days prior.

The third parties the disputed payments were made to were new payees. Barclays has shown us that, to set up new payees via mobile banking, the security number on Mr R's debit card would need inputting. As I pointed out, Mr R says his card hasn't been

compromised. I can't see how someone other than Mr R would've been able to obtain these details without his consent. So it seems most likely that Mr R, or someone with his consent created the new payees on his account.

Mr R remains adamant that his device was hacked by a fraudster. He says he spoke to a third-party telecommunications company that gave him information about how fraudsters could've accessed his device. However, neither Mr R or Barclays have given me evidence which shows Mr R's phone was likely hacked or was being used through other remote methods by fraudsters.

For his device to have been hacked, there needs to be a clear point of compromise that I can point to. A fraudster is unlikely to be able to hack into Mr R's phone without some sort of action on his part. But Mr R confirms he hasn't had any suspicious emails or messages, his banking information isn't written down anywhere and his phone hasn't been accessed by anyone other than himself. So there doesn't seem to be a clear point of compromise that would allow a fraudster to hack into Mr R's phone.

So it's difficult for me to fairly conclude that Mr R's device was hacked in the way he says it was. I also think it's unlikely an unauthorised individual was able to carry out the transactions without having actual access to the device, Mr R's banking app and the passcode for it, as well as his debit card.

Mr R suggests his information may have been compromised when he enquired about making a loan application around February 2022. He says he became suspicious of the information he'd been asked to provide and decided not to go any further. But this doesn't suggest his phone was compromised at the time nor does it provide an explanation of how someone was able to obtain his card details and the details needed to raise the indemnity claims, as well as create new payees. I also think it's unlikely that a potential fraudster would wait several months to fraudulently remove funds from Mr R's account.

The pattern of activity with the disputed payments also makes me think it's unlikely Mr R's phone was hacked. The disputed payments were carried out over different days and tend to follow on shortly after funds credited Mr R's account. This would've required regular monitoring of Mr R's account, which I find is unlikely. Moreover, this isn't typical of the opportunistic activity of a fraudster – which is to quickly maximise the fraudulent removal of funds in one instance.

In conclusion, despite what Mr R has said, the information I've seen makes me think it's most likely that Mr R, or someone with his consent carried out the disputed payments. I empathise with Mr R, given he's been pursued for the funds related to the indemnity claims. But I'm not persuaded that Mr R didn't authorise the payments he now disputes.

My final decision

For the reasons above, I'm not upholding this complaint.

Under the rules of the Financial Ombudsman Service, I'm required to ask Mr R to accept or reject my decision before 18 December 2023.

Abdul Ali
Ombudsman