DRN-5036311

The complaint

Mrs K complained because Lloyds Bank PLC refused to refund her for transactions she said she didn't authorise.

What happened

On 5 May 2024, Mrs K rang Lloyds. She said that there had been two outgoing bank transfer payments that morning, totalling £6,185, which she hadn't authorised. Mrs K said she had biometric security on her phone and banking app, and hadn't received any strange calls, and hadn't disclosed her details to anyone.

Shortly before the two outgoing payments, a £5,000 credit had come into Mrs K's Lloyds account from Mrs K's account with another bank. There wouldn't have been enough in the Lloyds account to pay the disputed transactions without this credit.

The next day, 6 May, Mrs K rang again. She said that a couple of months ago, she'd called to report her phone stolen, and had her card replaced. She said she thought whoever stole her old phone, which had face ID, had now hacked into her Lloyds account.

Lloyds checked. Mrs K had phoned Lloyds on 30 March. But the call recording showed that Mrs K hadn't said her phone had been stolen. What the call recording showed was that Mrs K had said she'd cancelled her card on her banking app. The computer records show she had done that. In the 30 March call, Mrs K had told Lloyds it was a mistake to have cancelled her card, and she'd asked Lloyds stop this.

Mrs K had also registered an additional phone on her Lloyds account at 12.40pm on 30 March.

The adviser said that there was no record of Mrs K having reported her phone stolen, only asking for a card replacement. He commented that there was face ID on her phone and the alleged fraudsters had waited two months before trying to use the phone. Mrs K was very unsure about some of her answers, including when she'd lost her phone, and when she'd registered the Lloyds app on her new phone. At the end of a long call, the adviser said that taking into account the information on its systems and what Mrs K had said, Lloyds had nothing to suggest the transactions had been carried out by someone who had fraudulently obtained Mrs K's details.

Mrs K complained, about not being refunded and about Lloyds' service.

Lloyds sent its final response letter on 6 June. It said that the payments had been made using Mrs K's genuine details. And during the investigation, Mrs K had told Lloyds that she'd clicked on a link and had entered her phone ID, and Lloyds sort code and account number. Mrs K had said she believed this was how the payments had been made.

But Lloyds said that the payments had been made using fingerprint or face ID on the device Mrs K had previously registered. Mrs K had previously said that no-one knew her banking

details and her device was protected. So Lloyds said it wasn't possible for anyone else to have made the payments. It did, however, pay her £30 for service when she'd phoned.

Mrs K wasn't satisfied and contacted this service.

Our investigator didn't uphold Mrs K's complaint. Mrs K had said that her phone had gone missing on 30 March when at a self-checkout at a shop between 1 and 2pm. The investigator pointed out that Mrs K had registered a new phone for Lloyds' online banking at 12.40pm. So she'd bought the replacement phone and registered it before the old one had been stolen. Nor had she told Lloyds that her phone had been lost when she rang Lloyds that day.

Mrs K also hadn't been able to provide a copy of the fraudulent text message which she said had led to her disclosing her details. And as Mrs K's phone had been protected by biometrics, the investigator couldn't see how anyone who'd obtained the old phone could have used it to make the disputed transactions.

The investigator also pointed out that the payments had been funded by a £5,000 payment into Mrs K's account shortly before the payments, and that the evidence showed that Mrs K had used her new phone to log in to her Lloyds online banking between the two disputed payments.

Mrs K wasn't satisfied. She asked for an ombudsman's decision, and said she had further points to make.

Mrs K said she'd now realised that it wasn't 30 March when her phone had been stolen, but 24th. She said the phone had been unlocked when stolen, so someone could have seen her put her code in when she'd paid, and would then have been able to have access to all her bank details. She said that as she had unwittingly not told Lloyds about the theft, an opportunist thief would have taken advantage of this.

Mrs K also said that the reason she'd logged in between the two disputed transactions was that she'd had an alert, so she wanted to check quickly. Mrs K said only the thief could know why they'd then waited several weeks rather than stealing the money straightaway when they stole the phone.

Our investigator replied that although Mrs K had said her phone had been unlocked when stolen, Mrs K had previously said that her husband had tried to ring the phone at that time and it was turned off. The investigator also pointed out that biometrics were needed to access the phone.

Mrs K then said that her other bank, from which the £5,000 transfer had been made into her Lloyds account, had said that the transfer had been made from an IP address (a unique computer identifier) which was abroad.

Mrs K's complaint was passed to me for an ombudsman's 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.

There are regulations which govern disputed transactions. The relevant regulations here are the Payment Services Regulations 2017. In general terms, the bank is liable if the customer didn't authorise the payments, and the customer is liable if they did authorise them. The

regulations also say that account holders can still be liable for unauthorised payments under certain circumstances – for example if they've failed to keep their details secure to such an extent that it can be termed *''gross negligence.''*

So what I have to decide is whether I think it's most likely that Mrs K, or a third party fraudster, authorised the disputed transactions.

The technical evidence shows that the two disputed payments were made using the device which Mrs K had previously registered to her Lloyds account. This device was protected by biometrics. So I can't see how a third party fraudster could have made them.

In Mrs K's recent additions to her evidence, she's said that the phone was open when it was stolen from her at a shop. She's also recently changed when she said that theft occurred, saying it was 24 March not 30 March. But if her phone really had been open, with the biometrics and Lloyds app open when it was stolen, I'd expect fraudulent transactions to have happened immediately. It's just not probable that fraudsters would have waited such a long time until the alleged text link message on 20 April, and a further long wait until the disputed transactions on 5 May. That's both because a fraudster would want to maximise their gain immediately, and also because by then the phone would have needed Mrs K's biometric details and Lloyds app security entering again.

I've also noted that there are no transactions, either on 30 March or 24 March, from Mrs K's Lloyds account to the retailer she said she was paying, with her phone and Lloyds app open, when her phone was stolen.

I also can't understand why Mrs K didn't report her phone stolen to Lloyds, either in the call on 30 March if that's when the alleged theft happened, or why she didn't ring to tell Lloyds about the loss on 24 March, if that's when the alleged theft happened.

When our investigator pointed out that Mrs K also checked her online banking between the two disputed transactions, Mrs K said that this was because she'd had an alert. The first disputed transaction took place at 9.18am on 5 May. Mrs K logged on at 9.38. But she didn't phone Lloyds immediately to report a dispute. It was nearly an hour later, at 10.17am, when she rang Lloyds. I think anyone seeing a large payment they hadn't made would have phoned their bank sooner.

The disputed payments were only possible because of a £5,000 credit from Mrs K's own account with another bank, which credited her Lloyds account shortly before the disputed payments. Without this credit, the balance would have been too low for the disputed payments to have been made. Mrs K has recently said that the sending bank told her the IP address for the transfer was abroad. But I don't consider this is relevant to the key facts in this complaint. I think it's more likely that Mrs K transferred the money from her other account herself, to enable the two payments from her Lloyds account.

I've also borne in mind that Mrs K has repeatedly changed her evidence about what happened, both to Lloyds and to this service, and she's given inaccurate information. To give just a few examples, she told Lloyds she'd reported her phone stolen when she rang on 30 March, but the call recording showed she didn't. She also changed her evidence about when the alleged theft at the shop had taken place, from 30 March to 24 March, after our investigator pointed out that Mrs K had registered her replacement phone before the old one was stolen.

Bearing all these factors in mind, I find that it's most likely that Mrs K carried out the disputed transactions herself.

Finally, I note that Lloyds paid Mrs K £30 compensation for service. I find that this was generous in all the circumstances of this complaint, and I don't require Lloyds to do more.

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 Mrs K to accept or reject my decision before 28 January 2025.

Belinda Knight
Ombudsman