

The complaint

Mr and Mrs H complained because Metro Bank PLC refused to refund them for £900 of withdrawals which were made from their account after Mrs H's phone was stolen.

What happened

Mrs H's phone was stolen on 7 April 2022. She said she was having a meal out, and someone she described as a "*scruffy woman*" approached her with a document which she put on the table in front of Mrs H. She was begging for money. Mrs H didn't understand her, because she was speaking broken English. Mrs H repeatedly told the woman to go away. Eventually the woman did leave, but Mrs H realised that she'd laid the document over Mrs H's phone, and when she'd left had taken Mrs H's phone with her. Mrs H chased after her but unsuccessfully.

Mrs H had a passcode for her phone, and a different passcode to access the mobile payment service, neither of which had she written down. She also said she had face recognition for both her phone and to access the mobile payment service.

On 8 April, several transactions were made from Mr and Mrs H's joint Metro account, using a mobile payment service on Mrs H's phone. Five payments took place at a superstore in quick succession, totalling £900. There were then three declined payments, for £300, £100 and £100.

Mrs H contacted Metro to dispute the transactions. However, Metro didn't contact Mrs H until 1 June, and when Mrs H rang Metro on 3 and 6 June, she was put through to the wrong team. By 8 August, Mrs H made a complaint, but Metro didn't raise a complaint for her.

In November 2022, Mrs H contacted this service. We got in touch with Metro, which started its complaint investigation. Metro said that it didn't uphold Mrs H's claim for a refund for the disputed £900 transactions, because whoever did the transactions would have done so using Ms H's biometric data and her passcodes. However, Metro acknowledged that it hadn't provided Mrs H with a good service because it hadn't made contact promptly, had mis-directed Mrs H's calls, and hadn't raised a complaint. It offered Mrs H £100 compensation for that.

Our investigator didn't uphold Mrs H's complaint. He said that all the disputed transactions had been made using the mobile payment service, which needed a passcode and optional biometrics to authorise any transaction. Mrs H had told him that she had a passcode which she hadn't written down anywhere, and that she didn't know how the person who had stolen her phone had been able to use it for the transactions.

So the investigator said that as there wasn't any point of compromise, he couldn't ask Metro to refund Mrs H. He thought Metro's offer of £100 was fair.

Mr and Mrs H didn't agree. Mr H explained that basically Metro was accusing his wife of fraud. He said that at the time of the disputed transactions, they'd been in the phone shop sorting out Mrs H's replacement phone. Mr H said they'd like the police to investigate,

because they lived a very honest life, and they were very unhappy that Metro was accusing Mrs H of fraud. The investigator told Mr H that this service can't ask the police to get involved, but he could ask for an ombudsman's decision. Mr H said he'd seen online articles about mobile payment services not being secure, and forwarded some of these to the investigator. The investigator asked if there was any more information about how anyone else might have obtained the necessary passcodes or biometrics, but Mr H said no, he was always very insistent to Mrs H that she should be careful about security, and even he didn't know her passcode. He also said they'd never shopped at the supermarket where the transactions had taken place. Mr H asked 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.

Regulations

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 say that the payment service provider (here, Metro) must show the transaction was authenticated. That's the technical part, and here, Metro should provide evidence that the transactions were properly authenticated. I asked Metro for full evidence, which it failed to provide. Unfortunately it does sometimes happen that this service doesn't have all the evidence we'd like. When that happens, I take my decision on the basis of what's more likely than not to have happened.

Here, I know the transactions took place on Mrs H's mobile phone, which she said was stolen. The transactions appear to have taken place in a supermarket. So I think it's most likely that whoever had the phone also had the log-in credentials, rather than any sort of online hack.

I've gone on to consider whether it's more likely than not that Mrs H authorised the payments. 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*."

Authorisation of the payments

I recognise that Mr and Mrs H feel strongly about their complaint, and are quite clear that they didn't carry out the transactions. But the problem here is seeing how the fraudster could have carried out the transactions. I asked Mrs H for more information about the security, to see if there was any way a fraudster could have obtained the information. I also asked how she thought any fraudster could have obtained her passcode. But she said she had no idea.

So Mrs H told us that:

- the phone had a passcode that only she knew, and it wasn't written down anywhere. It also had face recognition;
- the mobile payment service was protected by face recognition and she had memorised the passcode;
- the passcodes were different for the phone and for the mobile payment service.

In view of this, it's not possible for me to conclude that a third party fraudster carried out the transactions. That's because I can only do so if there's some reasonable explanation for how

the fraudster might have been able to do this. I recognise that Mr H has sent us links to various internet articles to indicate that mobile phones and mobile payment systems can be accessed by fraudsters. But there's also a lot of evidence to indicate that mobile phone and mobile payment systems are secure, provided the customer keeps their details private. And with biometric data being used, it's even harder to see how fraudsters could get round that. So I don't uphold Mr and Mrs H's complaint for the £900 of transactions.

Metro's service towards Mrs H

I've considered Metro's service towards Mrs H. As I've set out above, Metro has itself admitted that it didn't contact Mrs H in a timely way after she raised the fraud complaint in April 2022. It mis-directed her calls on 3 and 6 June, and ignored Mrs H's 8 August request to make a complaint. Metro didn't look at Mrs H's complaint until she raised it with this service in November 2022. That's a very long time, and it's understandable that Mr and Mrs H would have been frustrated and annoyed with Metro. So I consider it's right that Metro should pay Mr and Mrs H compensation for the distress and inconvenience caused by its poor service. I find that £100 is fair and reasonable.

My final decision

My final decision is that I uphold this complaint in part. I order Metro Bank PLC to pay Mr and Mrs H £100 compensation for distress and inconvenience caused by its poor service.

Under the rules of the Financial Ombudsman Service, I'm required to ask Mr H and Mrs H to accept or reject my decision before 24 May 2023.

Belinda Knight
Ombudsman