

## **The complaint**

Mr M complains that Barclays Bank UK PLC (“Barclays”) failed to refund transactions he didn’t recognise after his phone was stolen.

## **What happened**

### *What Mr M says*

Mr M explained that he was out with a friend and early in the morning when both their phones were stolen by unknown persons who drove away in a vehicle. Mr M said his was unlocked at the time.

Following the theft, Mr M believes the thieves managed to compromise the security of all his various banking apps including his Barclays Mobile Banking (BMB) app. It was later suggested that the thieves “jailbroke” his phone which accounted for access to the banking app.

A number of transactions were then made which Mr M denies knowing about totalling about £6,000. Another bank later refunded part of this, leaving about £4,000 in losses which Mr M asked Barclays to refund.

At the time of the theft, Mr M notified both the police and Barclays. He said that despite telling Barclays his account was compromised, they allowed further payments to leave his account. Later, Barclays declined to refund the money.

Mr M complained to Barclays about the loss of his funds, but they didn’t change their position about the refund and Mr M then brought this complaint to the Financial Ombudsman Service for an independent review.

### *What Barclays said*

Barclays’ fraud detection system noted payments leaving Mr M’s account on the day he said his phone was stolen. They carried out verification using various methods and at one stage spoke with a caller who said he was Mr M. That caller was able to pass security by providing details about Mr M including his place of birth.

A lengthy discussion about scams was held with the caller and a payment was cancelled at the caller’s request. Further payments were noted, and the caller made another smaller payment whilst on the phone using Mr M’s BMB app.

Later, further verification using a passport and driving licence were carried out before Mr M notified Barclays about the loss of his phone and the disputed transactions.

Barclays carried out an investigation into the circumstances and believed Mr M was responsible because the BMB app was accessed using a passcode known only to Mr M in conjunction with a biometric check (Face ID). They again declined a refund when he complained.

### *The investigation so far*

An investigator was assigned to look into Mr M's complaint and asked for evidence from both parties. Mr M provided details about his experience and evidence of reporting the loss to the police. Unfortunately, the police couldn't identify any evidence about the theft due to the lack of CCTV coverage and no UK link could be found to a suspect. He also provided information concerning contact with other merchants following the loss of his phone and evidence of a number of loans applied for in his name. Mr M had also confirmed that he hadn't had his passcode written down.

Barclays provided details of the use of Mr M's account and how his registered phone was used to access the account. This included details of which authentication method was used (passcode and Face ID).

Barclays were asked to identify if any unusual activity had taken place on Mr M's phone. They advised that they couldn't detect any attempts to subvert their banking app. They didn't believe that any other person could have used the app due to the biometric authentication process.

After considering the evidence, the investigator didn't uphold Mr M's complaint. He thought that because there was no plausible way for the BMB to be accessed, it was unlikely to have been anyone other than Mr M who was responsible for the disputed transactions.

Mr M disagreed with the investigator's outcome and asked for a further review of his complaint. As no agreement could be reached, Mr M's complaint has now been passed to me for a 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.

The relevant law surrounding authorisations are the Payment Service Regulations 2017. The basic position is that Barclays can hold Mr M liable for the disputed payments if the evidence suggests that it's more likely than not that he made them or authorised them.

Barclays can only refuse to refund unauthorised payments if it can prove Mr M authorised the transactions, but Barclays cannot say that the use of the Barclays Mobile Banking app (BMB) conclusively proves that the payments were authorised.

Unless Barclays can show that consent has been given, it has no authority to make the payment or to debit Mr M's account and any such transaction must be regarded as unauthorised. To start with, I've seen the bank's technical evidence for the disputed transactions. It shows that the transactions were authenticated using the payment tools issued to Mr M. I'll now need to consider the information provided by both parties to determine whether there's sufficient evidence to hold Mr M responsible for the disputed transactions or not.

Mr M's case is that his phone was stolen whilst in an unlocked state. Barclays notes say that he told them the thieves then drove off (with his and his friends' phones).

Barclays case is the disputed transactions couldn't have been without Mr M because they required both his passcode and biometric authentication (Face ID) to both access the BMB and then to authorise the payments from his account.

The process to access the BMB requires either a passcode or biometric authentication. Mr M

confirmed he hadn't given this (passcode) to anyone or had it written down on his phone. When looking at the circumstances of the reported theft, it's unlikely the thieves were able to gather the passcode for the BMB because they sped off after taking the phones. Mr M was told by another organisation that they could have accessed his BMB through "jailbreaking" his phone.

Whilst I can see that the thieves could access some parts of the phone because it was unlocked, I can't identify how they would be able to acquire the passcode known only to Mr M or replicate the facial biometric authentication. The BMB has its own security and would be unlikely to allow access just because someone had the phone.

I understand the suggestion about "jailbreaking", and could see how some aspects of the phone could be altered, but this doesn't account for how the thieves knew the passcode or were able to pass authentication with Mr M's biometric ID.

It's also apparent that two different people spoke with Barclays claiming to be Mr M. The voices are very different and assuming the person who called was the "thief" (because this call was about transactions that were later disputed), they had information about Mr M that was unlikely to be known to a random thief. They used this information to satisfy Barclays they were the genuine account holder after confirming security actions using the BMB which they'd already logged in to.

I accept that two different persons spoke with Barclays, but this doesn't automatically mean that Mr M wasn't responsible. The balance of the evidence shows that access to the BMB was unlikely to have been successful without Mr M's knowledge. That access was then used to make the payments that were later disputed. So, when I've assessed the overall evidence, I think it's more likely than not that Mr M was responsible for these transactions by allowing others to use his account, and it was reasonable for Barclays to hold him liable for them.

I understand this will not be the outcome Mr M wanted and he's strongly denied any involvement here, but I have to make my decision on what the evidence shows. In this case, that evidence shows there's no reasonable or plausible explanation for how the BMB was accessed by third parties. Without stronger evidence to the contrary – I'm unable to uphold 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 Mr M to accept or reject my decision before 22 September 2023.

David Perry  
**Ombudsman**