DRN-5177470

The complaint

Mr B, represented by a claims management company, complained because Barclays Bank UK PLC refused to refund him for transactions totalling £28,286.20. Mr B said his drink had been spiked and he didn't authorise the transactions.

What happened

At 7.38am, 7.39am and 8.31am on 25 February 2024, there were attempts to make a £1,200 payment on Mr B's card. Barclays' systems flagged these payments and declined them all.

Barclays then rang Mr B. Mr B correctly answered security questions, and the adviser explained he was ringing because there had been three attempts to make a transaction on Mr B's account which Barclays' fraud systems had blocked. He asked Mr B whether he'd authorised them, and Mr B said yes. The adviser asked what the transaction had been for, and Mr B said it was a transaction to a friend. The adviser asked if Mr B had used that merchant before, and he said yes. The adviser asked whether anyone had put Mr B under pressure to make that transaction, and Mr B said no. The adviser also gave Mr B security advice, saying that there were a lot of fraudsters trying to pretend they were a bank, and said that Barclays would never ask a customer to transfer money to a ''safe account'', to purchase goods, or to withdraw cash. The adviser also explained other things that neither Barclays nor genuine police officers would ask customers to do.

The adviser then said that he'd remove the block on Mr B's account as Mr B had confirmed he was happy with the transaction, and the account would be back up and running within about 15 minutes. Mr B thanked the adviser and the call ended.

Starting with a £1,000 payment at 9.45am the same morning, and ending with an £11.20 taxi fare at 21.24pm, there were then 10 payments from Mr B's account. A number of these payments were to the organisation to which the early payments had been attempted and which Mr B had confirmed to Barclays he'd genuinely attempted.

The payments between 9.45am and 21.24pm totalled £28,286.20.

In another call that morning, Mr B rang Barclays to transfer £5,000 from his Barclays account to an account with another bank, to which he'd transferred money before. Mr B passed multiple security questions, and also correctly provided the code which the adviser sent to Mr B's registered phone. The payment was then made as Mr B had requested.

On 27 February, Mr B rang Barclays and said he wanted to report fraud on his debit card. He said he'd been out with friends and had been quite drunk, and he'd gone to a party and he didn't remember where it was. He didn't remember anything which had happened, and substantial debits had been made from his account.

Barclays advised Mr B to contact the police, and investigated. It asked Mr B more questions. In reply, Mr B said he last remembered using his phone in the early hours of 25 February but he couldn't remember the time. He couldn't remember when he'd last used his card, because he believed his drink had been spiked and he had no memory of the night. He

didn't know how anyone else would have known his PIN, or his Barclays app passcode. He said his phone and card had been returned to him, but he didn't know when. He also said his friends had left by this time, but he'd met some other people he'd stayed with. He said that he had no memory of the night, and he just knew that when he woke up he was nearly home, and had his phone and card. He believed his drink was spiked and a fraudster had managed to access his Barclays mobile banking without his consent.

Barclays refused to refund Mr B, and he complained. In Barclays' final response letter on 21 May, it said that it understood Mr B had said he couldn't remember the time of the disputed spend, because he believed his drink had been spiked. Barclays said that its systems had detected some of the disputed spend, and had sent a text message for Mr B to confirm it was a genuine transaction. Mr B had replied, saying yes it was genuine. And Barclays said that it had also phoned Mr B to confirm recent activity and he'd confirmed he was making the payments, and no-one else had been telling him to make them. It said the call recording showed that Mr B had been coherent, and had answered all the questions Barclays had asked him. So this indicated Mr B knew about the payments being made.

Barclays' final response letter also said it hadn't been able to identify how Mr B's PIN had been compromised. The last genuine chip and PIN transaction had been six days earlier – so there hadn't been any opportunity for a potential fraudster to have watched Mr B entering his PIN.

Barclays also said that the terms and conditions of Mr B's account said he was responsible for keeping the card safe, and the PIN secret. The PIN had been correctly entered first time. Barclays could also see that Mr B had logged into his Barclays mobile banking throughout, using the correct passcode and biometric data – which again indicated Mr B had known about the disputed spend. So it said it hadn't been able to identify any third party involvement, and was holding Mr B liable for the spend.

Mr B had also reported a negative impact on his mental health. Barclays said it was sorry to hear that, and provided information about some organisations he could ask for help.

Mr B wasn't satisfied by Barclays' final response. Using a claims management company, he contacted this service.

Our investigator didn't uphold Mr B's complaint. She said that the genuine card and registered mobile had been used for the transactions. She listened to the calls between Barclays and Mr B, including when Barclays had phoned him on 25 February and he'd confirmed the declined payments had been genuine. She said that she agreed with Barclays that on those calls, Mr B had sounded coherent and of sound understanding. The investigator also said Mr B had felt his PIN had been obtained through ''shoulder surfing'' (someone watching him enter his PIN), but he hadn't used his card and PIN earlier that day, so that wasn't likely. And Mr B had been accessing his mobile banking app at the time when he said he'd been spiked, which meant his mobile passcode and banking app passcode would also have needed to have been compromised. So the investigator thought Barclays had reasonably concluded that it was more likely than not that Mr B had authorised the transactions himself.

Mr B's claims management company asked for copies of the call recordings. The investigator checked with Barclays, and with Barclays' consent, sent these to Mr B's representative.

Mr B, represented by the claims management company, didn't accept the investigator's view. The claims management company said that the phone call recordings indicated that Mr B didn't understand simple questions and fundamentally lacked mental capacity sufficiently

to authorise the payments. It said that when Barclays had asked Mr B to confirm his email address, Mr B had been unable adequately to answer the question. It also said that when Mr B had confirmed to Barclays that he'd used that merchant before, Barclays shouldn't have taken this at face value, and the claims management company hadn't seen evidence that Mr B had used the merchant before. It said Barclays should have questioned Mr B further, and if it had done, it would have discovered that Mr B didn't know the merchant and wasn't of sound mind to authorise the payments.

In regards to Mr B's PIN, the claims management company said that Mr B had told them he used the same PIN for his card as for his phone passcode, which was unlocked multiple times during the night. So it said this was likely to be how the fraudsters obtained Mr B's phone passcode which they then used for Mr B's PIN.

Mr B, represented by the claims management company, 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, and Terms and conditions

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.''*

There are also Terms and Conditions for Mr B's Barclays account, to which he agreed when opening the account. Section 2, ''*Keeping your money safe''* says

*''**You must look after your account access information***
You use payment tools to access your accounts and make payments. All these tools are personal to you.
***You must do all you reasonably can to keep your payment tools safe**.*
You must look after all the ways of taking money from or accessing your account. If we think any of your payment tools, such as cards, may have been compromised, we may send you a replacement to help keep your account secure.
***You must not give your payment tools to anyone else**.*
If someone takes money from your account because you have not kept your payment tools safe or secret when you should have done, you may lose all the money.

And section 6 ''*If someone takes an unauthorised payment from your account''*, also says:
''*You won't be entitled to a refund if you have acted fraudulently or you have deliberately or with gross negligence done the following things.*
• *You didn't keep your payment tools secure…''*

So what I have to decide is whether it's more likely than not that Mr B, or a third party fraudster unknown to him, carried out the disputed transactions. If it's likely to have been a third party fraudster unknown to Mr B, I also need to consider whether Mr B fulfilled his obligations to keep his security information private and secure.

Who is most likely to have carried out the disputed transactions?

To inform my decision, I've looked at the relevant computer records, including those about the disputed transactions, and the log-ons to Mr B's mobile banking app. I've also listened to the call recordings.

The call recordings include the two on the morning of 25 February which I've set out above. One was when Barclays blocked Mr B's card because of the three attempted payments at 7.38am, 7.39am and 8.31am. In this, Mr B confirmed those attempts were genuinely his. The other was when Mr B rang Barclays to authorise the £5,000 payment to another bank – a transaction he hasn't disputed.

I don't agree with Mr B's claims management company that on the call about the three attempted payments, it should have been clear to Barclays that Mr B *''fundamentally lacked mental capacity sufficiently to authorise the payments.''* The claims management company said that Mr B wasn't able to confirm his email address which proved this. But on the call, Mr B had already correctly answered his full name, which included four names, and his date of birth. The adviser then asked *''Can you confirm the email address we hold for you*?'' Mr B answered ''yes'', rather than giving the address. But when the adviser clarified the question, Mr B gave the correct email address. He then went on correctly to answer another security question. I can't agree that this showed clear lack of mental capacity.

Similarly, I don't agree with Mr B's claims management company that when Mr B replied to a question saying he'd used the merchant before, Barclays should have looked further into this. It didn't have any reason to disbelieve what Mr B had said. And even if Mr B hadn't used his Barclays account to pay the merchant on a previous occasion, he might have paid the merchant before using one of his other credit or bank cards with other financial organisations.

I also find that Mr B sounded very much the same on the two calls that morning, one of which was initiated by Mr B to authorise a transfer which he's never disputed. I consider it's highly unlikely that Mr B had mental capacity for the call where he authorised a £5,000 transfer which he didn't later dispute - but lacked mental capacity for the other call where he confirmed as genuine the transactions which Barclays had blocked for potential fraud checks.

Banks have to balance the needs of security with the need to ensure that customers' genuine payment instructions are carried out in a timely way. I don't consider there was anything in Mr B's voice, answers or manner which should have led Barclays to assume he lacked mental capacity and to block all future payments. And it had blocked three payments, only to be told by Mr B that these had been genuine. I've also borne in mind that some of the transactions which Mr B subsequently disputed were to the same merchant discussed in the three blocked payments which Mr B had confirmed to Barclays as genuine.

Looking at the disputed transactions, the technical evidence shows that whoever carried these out had Mr B's genuine card and correct PIN. Mr B suggested to our investigator that the fraudster had ''shoulder surfed'' him – in other words, saw him entering the PIN at a previous chip and PIN transaction. But there hadn't been any of these in the previous six days, so it wasn't possible for a fraudster on that day to have shoulder surfed Mr B.

After the investigator pointed this out in her View, Mr B's representative then said that Mr B had said his PIN for his card was the same as for his phone, and a fraudster could have seen Mr B enter his passcode during the evening, and then tried this as the card PIN. But if Mr B allowed someone to see him entering his passcode, he wasn't keeping his details secure. So I'm not persuaded by this argument.

Also, there are 10,000 possible combinations of a four digit number. So it's most unlikely that a fraudster could have correctly guessed the card PIN at the first attempt, and the records show there were no incorrect PIN attempts.

Mr B's mobile banking app was logged into repeatedly during the time of the disputed transactions. If this was done by a third party fraudster and not Mr B, the fraudster would have had to have had to have known Mr B's Barclays passcode, which he had a responsibility to keep secure. And logging into the app also required Mr B's biometric data.

So I can't see how a third party fraudster who might theoretically have stolen Mr B's card and phone, could have known the PIN and passcode to access and make transactions on Mr B's account, or access the app using Mr B's passcode and biometric data. But even if a third party fraudster had somehow done this, I find it's most unlikely that they'd have returned the card and phone to Mr B, who still had both the card and phone at the end of the disputed transactions. Firstly, there was still a significant amount of money in Mr B's account, and fraudsters don't typically leave money in an account. Secondly, there would be no reason for a fraudster to take the security risk of returning a card and phone, when they might be found out.

For these reasons, I find it's most likely that Mr B carried out the disputed transactions himself. This means Barclays doesn't have to refund him.

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 B to accept or reject my decision before 10 March 2025.

Belinda Knight
Ombudsman