DRN-4364583

The complaint

Mr A and Mrs H complain that Barclays Bank UK PLC ("Barclays") failed to refund transactions they didn't recognise.

What happened

Mrs H was mainly involved with this complaint, so I'll refer to her for ease of reading.

What Mrs H says

Mrs H said that she first noticed unusual activity on her account whilst out shopping. After checking her account, she noticed numerous payments had been made to various crypto currency merchants.

Mrs H called Barclays about the payments and told them she knew nothing about them. She mentioned it may be to do with a scam linked to a different bank. After going through the transactions (which were all made with her debit card), Barclays replaced her card and arranged for a temporary refund whilst they looked into the situation.

Later, Barclays told Mrs H they would be taking the refund back and they held her responsible for the payments. Mrs H complained and Barclays continued to investigate the matter. They didn't change their position and maintained that Mrs H was responsible for the payments.

Mr A and Mrs H then brought their complaint to the Financial Ombudsman Service for an independent review. An investigator was assigned to look into what had happened and asked both parties for information about the circumstances.

Mrs H said she'd only noticed the payments leaving her account whilst out shopping and believed that a scam she'd been caught up in was also responsible for these payments leaving her account. Mrs H said that she'd previously downloaded software that gave control of her devices to the scammer. Mrs H confirmed that she hadn't given her card or its details to anyone else to use. There were no other persons who could have obtained it and she hadn't lost it.

Barclays responded with information concerning the payments and how they were made, they also sent phone calls they'd had with Mrs H, including one that occurred during the period when the disputed transactions were taking place. They commented that the call (Mrs H was enquiring about additional credit/loan) didn't mention anything about unusual payments leaving her account despite regularly logging on to her banking app.

Barclays evidence in summary was:

- There was no evidence of any third party activity.
- The disputed transactions took place over an extended period of time.

- Mrs H's device was used to confirm some of the payments using additional security steps.

- Funds were paid into the account prior to the disputed transactions.

- There were multiple log ins to the mobile banking app during this period – but no mention to Barclays at the time.

- No further attempts to use the debit card after it was cancelled.

After reviewing the evidence, the investigator thought it was likely that Mrs H was responsible for the payments herself and didn't uphold the complaint. The investigator couldn't find any explanation to how Mrs H's card details were compromised, even if someone had remote access to her device.

Mrs H disagreed and asked for a further review of her complaint which has now been passed to me for a decision.

Mrs H provided copies of messages she'd had with a scammer and screenshots of crypto accounts where some of the disputed transactions were sent.

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.

Mrs H has described being caught up in a crypto currency scam and believes that after allowing remote access to her phone, the scammers took funds from her account without her knowledge or permission. Essentially she's denied authorising these payments.

The relevant law surrounding authorisations are the Payment Service Regulations 2017 and the Consumer Credit Act 1974. The basic position is that Barclays can hold Mrs H liable for the disputed payments if the evidence suggests that it's more likely than not that she made them or authorised them.

Barclays can only refuse to refund unauthorised payments if it can prove Mrs H authorised the transactions, but Barclays cannot say that the use of the card details for online payments 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 Mrs H'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 Mrs H. I'll now need to consider the information provided by both parties to determine whether there's sufficient evidence to hold Mrs H responsible for the disputed transactions or not.

These payments were made using Mrs H's debit card. She's confirmed she never gave the details of it to anyone else. So, it's difficult to see how those details were obtained, even if a scammer had access to her mobile phone. I would also note that no evidence had been provided regarding this remote access, so I can't say for sure if anyone had obtained access to her phone/device. Barclays themselves also couldn't find any evidence that a third party had obtained access.

I noted that on several occasions prior to the disputed transactions leaving the account, funds were paid into it to enable these transactions to be made. The disputed transactions were made over about nine days and other undisputed activity also took place during this time. On the face of it, the payments were funded from other accounts. It seems unlikely to me that a scammer would be able to access several different accounts and transfer funds to then spend it on crypto currency using a debit card that no one else knows about.

If it was possible that a scammer had access to the account(s), they could have taken the whole balance without going to the trouble of making debit card payments that also needed Mrs H to confirm using additional authentication steps. Barclays evidence is that some of the payments recorded Mrs H's registered mobile device, from a known IP address accessing the phone to confirm some of the payments to the crypto merchants.

Note: IP addresses are a means to identify physical locations that online transactions are connected to and can be the actual physical location or other locations connected to the provider of the data services.

Mrs H also provided details of a crypto account showing some of the payments she denied making. Her case here is that they weren't made by her, so I can't see how she would have details of an account if it was set up by a scammer to steal money from here. It seems to me that she would only have access to it if she herself opened it. I've also looked through the second complaint linked to the scam and couldn't see any payments to this particular crypto merchant. So, my conclusion would be that Mrs H had control of it which would be unlikely if it belonged to a scammer.

Mrs H also called Barclays to discuss a loan/credit card during the nine-day period of disputed transactions and no mention was made of unusual payments from the account. Mrs H was calling because she said she was in debt, so I would have thought, based on her regular use of her mobile banking app, that she would have been aware of the money being transferred into her account and the raft of payments leaving it.

Overall here, my objective assessment of the evidence is that I think it's more likely than not that Mrs H was responsible for making these payments and it was reasonable for Barclays to hold her liable for them.

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 A and Mrs H to accept or reject my decision before 13 November 2023.

David Perry
Ombudsman