DRN-4920143

The complaint

Mrs A complains that Barclays Bank UK PLC won't reimburse her after she fell victim to a safe account scam.

What happened

Mrs A has explained that she received a call from an individual purporting to work for Barclays, querying whether Mrs A had made particular transactions on her account. When Mrs A confirmed she hadn't, she was told her account at risk and that she should move her funds to another safe account. Unfortunately, unknown to Mrs A at the time, the individual she was speaking to was in fact a fraudster.

Mrs A has advised that she asked the fraudster how she can be sure they worked for Barclays and was told to ask the fraudster a question. Mrs A says she asked the fraudster for her mother's maiden name, which the fraudster was able to confirm. On this basis, she believed the call to be genuine and proceeded with the fraudster's requests.

Mrs A was advised that she should move all her funds to an account with another banking provider that she already held and from there, on to the safe account. Mrs A has explained that the transfer was made over several smaller payments, as requested by the fraudster. She said the fraudster also told her to move money from her Individual Savings Account (ISA) but she didn't wish to do that as she'd lose her the interest on the account. In total, Mrs A made the following three payments from her Barclays account:

Payment date	Payment value
29/12/2023	£600
29/12/2023	£550
29/12/2023	£446.72

Mrs A has explained that she was told to go onto her Barclays phone app and was directed on what to do. During the process of the scam, the fraudster was also able to set up another device that was linked to Mrs A's banking app.

Mrs A explained she was told what to do from her other banking account once funds had been moved to there, and that she transferred the funds to an account in an individual's name who she believed was an account manager. The fraudster advised Mrs A that they would call the following morning at 9:00, but when this didn't happen, Mrs A began to feel suspicious and contacted Barclays.

At this point she realised she'd fallen victim to a scam and raised a claim with Barclays.

Barclays considered Mrs A's complaint but didn't uphold it. It said that as funds were sent to another account in her name - that she had sent funds to before - it wouldn't be liable for her losses.

Mrs A remained unhappy and referred her complaint to our service. An investigator considered Mrs A's complaint but didn't uphold it. He didn't think the payments were sufficiently unusual that Barclays ought to have intervened, prior to processing them. He also considered that there was no real prospect of Barclays recovering Mrs A's funds, as she confirmed herself that they were moved on from her other banking account shortly after the transfer from her Barclays account.

Mrs A disagreed with the investigator's view and argued that it was the fraudsters, not her, that made the payments from both of her accounts. She considers that while the fraudsters were regularly putting her on hold during the scam call, they were gathering details from Mrs A's banking providers to enable them to make the payments.

The investigator considered further calls provided by Barclays which he shared with Mrs A also, but this didn't change his opinion. He said that during the calls at the time with Barclays, Mrs A made several references to being walked through the payment journey and being told what to do and say. While the investigator acknowledged that another device had been added to Mrs A's banking app, he confirmed that all evidence suggested the payments themselves were made from Mrs A's previously registered device.

Mrs A disagreed. She referenced a section of a call with Barclays where the advisor told her a device had been added to her account and she confirmed this wasn't her. She maintained that this was evidence that her account had been hacked.

As Mrs A disagreed with the investigator's view, the complaint has been referred to me for a final 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.

Having done so, while I'm sorry to disappoint Mrs A, I'm not upholding her complaint. I appreciate this isn't the outcome she was hoping for, but I've explained my reasons for reaching this outcome below.

I've first considered Mrs A's complaint that she didn't make or authorise these payments and that they were made by the fraudster. Having considered the available evidence I can see that a new device was added to Mrs A's account at the time this scam happened. However, Barclays has provided more detailed audit records that show what specific devices completed the transactions in question and I can see that the device ID listed as completing the disputed transactions is the same one used to make genuine, undisputed payments both pre and post scam. While I can see the fraudster used the new device to login to Mrs A's account, there's nothing to suggest this device was involved in making any payments. Additionally, Barclays has confirmed the process required to add a new device to an individual's banking app, which includes Mrs A being provided with a code that she would have been required to share with the fraudster. I can also see that the new device was added to Mrs A's banking app within around 30 minutes of the first payment being made from her account towards the scam. So I think it's most likely that Mrs A was tricked into sharing information during the call that allowed the fraudsters to access her banking app, rather than her account having been hacked, particularly as she's mentioned being left waiting on hold for extended periods during the call.

Additionally, while I appreciate memories fade over time on specifically what happened during the scam, Mrs A's calls with Barclays shortly after the scam support that it was her that made the payments. For example, during the calls, Mrs A said *'they wanted me to move my ISA money as well and I said sorry, no… I'm going to lose interest'*, which I think supports the idea that it was Mrs A ultimately in control of making the transfers, even though the fraudsters may have had an overview of her accounts from a separate device, as they otherwise could have moved money from her ISA without her permission. When asked why Mrs A made three smaller value payments to her other account provider rather than in one lump sum, she also said that it was what she was told to do. Similarly when explaining the process, Mrs A said '*what I remember is them saying go into your Barclays account… and then you can do a transfer to your [other provider's] account.'* This all supports the available evidence that it was ultimately Mrs A making the transfers, albeit under the guidance of a fraudster.

I therefore think it's more likely than not that while another device was added to Mrs A's account, this was done in order to make the scam appear more realistic, for example, having a better oversight of Mrs A's accounts and balances. I've not seen evidence that suggests it was this additional device that made any payments from Mrs A's account. I therefore think Mrs A authorised the payments.

However, this isn't the end of the story. I've gone on to consider whether Barclays should be held liable for Mrs A's losses based on any other obligations it has to her.

In broad terms, the starting position at law is that firms are expected to process payments and withdrawals that a customer authorises it to make, in accordance with the Payment Services Regulations (in this case the 2017 regulations) and the terms and conditions of the customer's account. However, where the consumer made the payment as a consequence of the actions of a fraudster, it may sometimes be fair and reasonable for the bank to reimburse the consumer even though they authorised the payment.

The Contingent Reimbursement Model (CRM) Code can provide additional protection for the victims of APP scams such as this was. However, payments made to another account belonging to the scam victim are not within the scope of the CRM Code. So I cannot fairly apply the terms of the CRM code to any of the payments Mrs A has made.

However, taking into account relevant law, regulators rules and guidance, relevant codes of practice and what I consider to have been good industry practice at the time, I consider it fair and reasonable that Barclays should:

- have been monitoring accounts and any payments made or received to counter various risks, including preventing fraud and scams;
- have had systems in place to look out for unusual transactions or other signs that might indicate that its customers were at risk of fraud (among other things). This is particularly so given the increase in sophisticated fraud and scams in recent years, which firms are generally more familiar with than the average customer;
- in some circumstances, irrespective of the payment channel used, have taken additional steps, or made additional checks, or provided additional warnings, before processing a payment.

It isn't in dispute that Mrs A has fallen victim to a cruel scam here - but I've thought about whether Barclays should have reasonably intervened prior to processing the payments.

Mrs A was making payments to an account in her own name, that she made regular payments to. Therefore while the scam payments were higher than her usual payment

transfers, they weren't so out of character that I think this ought to have raised concerns with Barclays. Additionally, I think the perceived risk here from Barclays' perspective would've been relatively low, even with slightly higher payment values, as she was paying a trusted and established account of her own. I've taken into account that a new device had recently been added to Mrs A's account and this could be considered a potential flag for fraud. However, as the evidence suggests that payments weren't made from this device, when combining this with the factors mentioned above, I simply can't conclude that Barclays acted unreasonably in allowing these payment transfers to be processed without additional intervention.

Recovery of funds

Lastly, I've considered whether Barclays did all it could to recover Mrs A's funds once it was made aware of the scam. Given Mrs A made the payments to her own account held with another firm, I'm not persuaded there's anything Barclays could have done to recover her funds as this would require Barclays to raise a fraudulent claim against Mrs A's own account.

Overall while I'm sorry to disappoint Mrs A – and I don't underestimate the impact this cruel scam will have had on her - I haven't determined that Barclays can be held responsible for her losses and I therefore don't require it to reimburse her.

My final decision

My final decision is that I don't uphold Mrs A's complaint against Barclays Bank UK PLC.

Under the rules of the Financial Ombudsman Service, I'm required to ask Mrs A to accept or reject my decision before 4 February 2025.

Kirsty Upton
Ombudsman