

The complaint

Ms S complains that Barclays Bank UK PLC (“Barclays”) won’t refund money she lost when she fell victim to an investment recovery scam.

What happened

Ms S fell victim to an investment scam in 2017. In 2020, she was approached by a company “R” who offered its services in recovering money she had previously lost.

Between January 2020 and June 2021, Ms S sent over £80,000 to R from her Barclays bank account. The funds were first sent to a cryptocurrency exchange for conversion into cryptocurrency, before being sent on to cryptocurrency wallets as instructed by R. Unfortunately, Ms S had fallen victim to a scam once again.

Our investigator didn’t uphold Ms S’s complaint. They explained that Barclays had blocked one of the earlier payments and questioned Ms S, and she had misled the bank about the true purpose of the payment. They went on to say that the chat messages between Ms S and the scammer showed that in the days following this, Ms S had attempted to make a payment from her account with another bank. But that bank became concerned that Ms S was being scammed and contacted the police. But she continued making payments from her Barclays account. Amongst other observations, the investigator noted that the scammer had coached Ms S into lying to the banks. They concluded that a subsequent intervention by Barclays would not have prevented her from going ahead with the payments.

Ms S doesn’t agree with the investigator’s findings. In summary, she says that the investigator’s outcome is heavily based on the chat messages provided. Ms S disputes some of the findings made by the investigator and explains that what she said to the scammer didn’t necessarily correspond with what happened.

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.

I’m sorry to hear about the impact this scam has had on Ms S’s health. I don’t doubt that losing even more money has made things difficult for her, especially where she’s borrowed money from others. I therefore realise that this will come as a considerable disappointment to Ms S, but I agree with conclusions reached by the investigator. And that means I’m not upholding this complaint. I’ll explain why.

Under regulations and in accordance with general banking terms and conditions, banks should execute an authorised payment instruction without undue delay. The starting position is that liability for an authorised payment rests with the payer, even where they are duped into making that payment. There’s no dispute that Ms S made the payments using her security credentials, and so they are authorised.

But in accordance with the law, regulations and good industry practice, a bank should be on the look-out for and protect its customers against the risk of fraud and scams so far as is reasonably possible. If it fails to act on information which ought reasonably to alert a prudent banker to potential fraud or financial crime, it might be liable for losses incurred by its customer as a result.

The first seven disputed transactions weren't flagged by Barclays's fraud detection system. Having reviewed the operation of Ms S's account, I don't consider the transactions – which happened between 9 and 21 January 2020 – as being particularly unusual or suspicious such that I think Barclays ought to have intervened. The amounts in question were in line with the usual account spending.

Barclays did flag a further payment on 21 January. According to its systems notes, a payment for £1,500 attempted at 12:37, to the merchant Ms S had been making payments to, was detected as unusual and blocked by the bank. The note goes on to state an attempt was made to call Ms S's mobile and a message was left asking her to call back.

There's a further note, which I've reasonably assumed is from when contact was ultimately made, which states that the transaction was discussed, and Ms S said she was paying a deposit for a car which she'd seen on an online car marketplace. The note goes on to say that the call was disconnected while the agent was still looking into this. And should she call back, to question Ms S further or ask her to go into a local branch with more information. Looking at the bank statement, the transaction in question for £1,500 to the said merchant didn't leave the account. This suggests that the payment was cancelled. A further note states that Ms S's identity was verified using her driving licence.

Ms S has disputed that a call took place between her and Barclays on 21 January. She's provided an itemised phone bill covering the relevant period to evidence that she didn't receive a call from anyone that day. I recognise that Ms S feels very strongly about this. I appreciate she's told us that she requested her mobile provider to provide a list of incoming and outgoing calls. But the itemised bill doesn't confirm that the calls listed include both incoming and outgoing calls. In my experience, it's not common for mobile phone providers to list incoming calls unless they incur a charge.

Even if I'm wrong about that, it's clear from the chat messages between Ms S and the scammer that she did receive a call on 21 January. And that she attempted to make a payment for £1,500, but it didn't go through. The timestamp on the bank's system notes matches that on the corresponding chat messages. At 12:34, the scammer told Ms S to *"put 1500"*. Six minutes later, she replied, *"I done but doesn't show went out from my account"*. At 13:59, Ms S tells the scammer, *"Bank is calling me and they really rud [sic] and asked many questions"*. 21 minutes later, at 14:20, Ms S says, *"They asking because of bitcoins and they said they will verify the account payee"*. At 16:08, Ms S tells the scammer, *"I'm now in Barclays to unblocked my account"*.

I'm therefore persuaded that Ms S attempted to make a payment for £1,500 which was blocked by Barclays and that resulted in a phone call which then led to her visiting the branch. Considering Ms S's recollections from the time aren't accurate, and the bank's system notes regarding the payment amount and branch visit do correspond with the chat messages, I'm persuaded that the other information recorded in those notes is also correct. Namely, that Ms S told Barclays the payment was to pay for a car deposit.

I understand that Ms S feels a lot of weight has been placed on her chat messages with the scammer. It's not that I discount a consumer's testimony altogether when deciding a complaint – it is evidence after all. But where evidence is missing or there's a dispute over what happened, it is my role to weigh up the information available and decide on the balance

of probabilities what is more likely than not to have happened. These events happened nearly four years ago. As I've been able to show above that Ms S's recollections aren't accurate, I've placed more weight on contemporaneous notes from that time, i.e., the bank's system notes as well as the chat messages which is a record of conversations between Ms S and the scammer as they were happening.

I can see that on the same day (21 January), the scammer also encouraged Ms S to transfer funds from her Barclays account to her account with another bank as a work-around to future blocks placed by Barclay. And while in branch to get the initial block removed, she transferred £8,000 to that account.

Ms S disputes attempting to make a payment to the scammer from that account. She submits that she hadn't received an activation code for online banking, and this prevented her from making transactions. But according to the chat messages, Ms S informed the scammer on 21 January that she had received a letter from the other bank with the code. And messages from around 16:45 that day do suggest that she tried to send £8,000 from her account with the other bank to the cryptocurrency exchange. But that transaction didn't go through, and Ms S had to phone the bank before being told to visit the branch.

Given this, I'm satisfied that the following day, when Ms S went into the branch of the other bank, its enquiries were about the cryptocurrency-related payment. Looking at the chat messages from that day, Ms S even tells the scammer that the branch had said 80% of people buying bitcoin had been scammed. What's more, it's clear from the messages that Ms S was being coached by the scammer into lying to the bank. I won't set out all the relevant conversations, given Ms S has a copy of the messages, but the scammer advised her not to tell the bank that someone was trying to help her. And to say that she had full responsibility over her money and every right to make the transaction.

Ms S's other bank wasn't satisfied with her answers and the police were called. But this doesn't appear to have stopped her as she resumed making payments from her Barclays account once again. I'm mindful that police involvement, which under circumstances would have more likely than not centred around the payment Ms S had attempted to make, didn't affect her decision-making. So, I'm not convinced that further questioning by Barclays when she made the subsequent transactions would have stopped her from going ahead either.

It is evident from the chat messages that during this time, Ms S had some suspicions of her own about the legitimacy of R. But she felt reassured by the scammer each time she questioned things. This includes an incident when a third-party contacted her and questioned the legitimacy of R as they thought they were being scammed.

What all this means is that I don't think Barclays could reasonably have done anything more to prevent or limit Ms S's losses.

I've also thought about recovery of payments when Barclays was notified of the situation. Only two of the disputed transactions were card payments. So, the investigator's finding on this point isn't relevant to the remaining payments. But I'm satisfied that this doesn't affect the outcome as I think recovery is unlikely to have been successful.

For the card payments, the only recourse would have been a chargeback. But it could have only been attempted against the merchant Ms S paid, i.e., the cryptocurrency platform, not a third party (the scammer). It's unlikely that a chargeback would have been successful given the merchant did provide the service that was requested (conversion of fiat money into cryptocurrency). As for the faster payments, the money was sent to Ms S's crypto wallet, which once converted into cryptocurrency was sent on to the scammer (although she didn't

know this at the time). Therefore, no funds would have been recoverable from the beneficiary (the provider of her crypto wallet).

In summary, I know that Ms S will be disappointed with this outcome. Not least because the matter has been ongoing for some time. I fully acknowledge that there's a lot of money involved here. Despite my natural sympathy for the situation in which she finds herself, for the reasons given, it wouldn't be fair of me to hold Barclays responsible for her loss.

My final decision

For the reasons given, my final decision is that I don't uphold this complaint.

Under the rules of the Financial Ombudsman Service, I'm required to ask Ms S to accept or reject my decision before 19 February 2024.

Gagandeep Singh
Ombudsman