

## The complaint

Mr and Mrs S complain that Barclays Bank UK PLC did not reimburse the funds they lost to a scam.

## What happened

Mr S was introduced to a cryptocurrency investment opportunity, that I will refer to as 'X' by a friend. He carried out some research and attended an online presentation, and met others connected to the investment opportunity in person at an event. When he was sufficiently persuaded by the opportunity, he made payments from his joint Barclays account with Mrs S as detailed below. The initial two payments were sent to individuals I'll refer to as 'F' and 'N' which he was told would be forwarded to X:

Date	Amount	Payee
07/02/2022	£7,838	F
23/02/2022	£23,511	N
19/04/2022	£7,920	Mr S' crypto account

Mr S did not receive any returns and in late 2022, X informed investors no-one was able to access withdrawals or rewards. Despite promises this was being rectified, no further withdrawals were allowed and Mr S lost his funds. He now feels he was the victim of a scam, and his representatives have said it is now widely accepted that X was operating a scam.

Mr and Mrs S raised a scam claim with Barclays via their representative, but Barclays responded in March 2024 to explain they needed additional evidence of the scam occurring before they could fully investigate. The complaint was referred to our service and our Investigator looked into it. They initially did not think there was enough evidence linking the payments listed above to X, so they did not think there was enough to be satisfied the payments were linked to a scam.

Mr and Mrs S' representative was able to provide some additional evidence. As a result, our Investigator issued a second view in which they set out they felt there was enough evidence to link the first two payments to X, but they still felt there was not enough to show the third payment was linked to a scam. For the first two payments, they did not think there was enough to show the payees had knowledge of the scam operation at X when the payments were made, so they did not think the Contingent Reimbursement Model ("CRM") Code could be applied to the payments. They also felt Barclays had done enough to try and protect Mr and Mrs S from financial harm when processing the payments, so they did not recommend reimbursement.

Mr and Mrs S disagreed with the findings, via their representative. In summary, they felt that the payments made to F and 'N' were ultimately linked to the scam so should be covered by the CRM Code. And they felt more robust warnings on payments 1 and 2 would have highlighted the payments were going to a scam and prevented further payments from being made.

As an informal agreement could not be reached, the complaint has been passed 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, I agree with the Investigator for largely the same reasons. I will set out my reasoning in more detail.

On balance, I do think Mr and Mrs S have been able to provide enough evidence to satisfy me that it's more likely payments 1 and 2 ultimately went to X. However, I have not been provided with any further evidence in relation to the final payment made directly to a cryptocurrency exchange. Mr S says he lost these funds, but I've not been provided with anything that shows how the payment was linked to any form of scam. With this in mind, I do not think it can safely be said this payment is linked to a scam, and I will not consider it further within this decision.

I've gone on to consider whether or not payments 1 and 2 are covered under the CRM Code. In this complaint, the payments weren't made directly to the scammer, in this case X. Instead, they were made to an individual and a company before being passed onto the scam. The CRM Code sets out the definition of an authorised push payment ("APP") scam:

*...a transfer of funds executed across Faster Payments...where:*

- (i) The Customer intended to transfer funds to another person, but was instead deceived into transferring the funds to a different person; or*
- (ii) The Customer transferred funds to another person for what they believed were legitimate purposes but which were in fact fraudulent.*

I am satisfied Mr S paid the individuals he was intending to pay, so I do not think the first point is relevant here. What is left to decide is if he transferred the funds to both F and N for what he believed was a legitimate purpose that turned out to be fraudulent. When considering this I have to determine what Mr S's purpose of the payments were, what both F and N's purpose were and whether they aligned. If they did not align, I need to think it's more likely this was down to dishonest deception on F and N's part. I essentially need to consider whether F and N were involved in and aware of the scam operation facilitated by X.

It appears that for both payments, Mr S intended for the funds to be forwarded to N and F so that they could pass them onto X as cryptocurrency. Mr S has said that he does not think F was aware of X being a scam at the point he was talking with her and sent her the funds. And none of the brief glimpses of communications I have seen suggest that she was any more involved than a facilitator of sorts. It appears that she received Mr and Mrs S's funds and helped him deposit them into his account with X, in line with what his intended purpose for the payment was. With nothing else to suggest she was more involved in the scam operation, I do not think the payment therefore falls under the protection of the CRM Code.

N was a business which was owned by an individual Mr S had met at an event held by X. This individual has been shown to be more involved in X's scam operation, but I have to consider that as a limited company, N is a separate legal entity to its owner. N itself has three separate directors, meaning it is not solely controlled by the individual with ties to X. The third-party bank which N has its business account with has provided me with the relevant statements for the period in question. While I cannot go into detail about what these show, there is no indication of a closer link with X than simply helping to facilitate Mr S's payment. Having carefully considered everything available to me, I think both Mr S and N's intended purpose for the payment aligned and I do not think this payment is covered by the CRM Code.

However, the regulatory landscape, along with good industry practice, also sets out a requirement for account providers to protect their customers from fraud and financial harm. And this includes monitoring accounts to look out for activity that might suggest a customer

was at risk of financial harm, intervening in unusual or out of character transactions and trying to prevent customers falling victims to scams. So, I've also thought about whether Barclay's did enough to try to keep Mr and Mrs S's account safe.

I have compared the two payments to Mr and Mrs S's genuine account activity, to see if they appear to be unusual or out of character. In doing so, I can see that Mr and Mrs S had made some higher value payments in the months leading up to the scam. As a result, I think the initial payment of £7,838 did not appear to be so suspicious that I think it warranted a human intervention from Barclays. I can see that Barclays did carry out an automated warning, and on balance I think this was proportional to the risk level the payment posed.

As a part of the automated warning, Mr S was asked to select what the purpose of the payment was. He selected 'Bill, Invoice or tax', and Barclays therefore provided a warning relevant to scams related to those kinds of payments. While I can appreciate this warning will not have resonated with Mr S, it was provided as a result of his selection so I cannot hold Barclays responsible for any error.

The second payment was for significantly more, and even considering the earlier high value payments I think a human intervention was warranted for this payment. I can see Barclays did intervene in this payment and spoke with Mr S on the phone to ask further questions about it. I have listened to a recording of this call and in it, Mr S was asked what the purpose of the payment was. Mr S said he was paying an invoice for courses which are provided by an individual he considers a friend and who he knows in person, and that he had paid them previously. As Mr S made no mention of an investment or cryptocurrency, and he said he knew the owner of the company he was paying personally, I think it is reasonable that Barclays did not probe further in relation to this payment. Mr S's answers did not bring up any red flags that may indicate he was falling victim to financial harm, and on balance I think the level of questioning matched the risk level of the payment itself.

I therefore think it is reasonable that Barclays did not meaningfully reveal the scam in the circumstances, and I do not think they therefore missed an opportunity to prevent further payments from being made.

I understand that this will be disappointing for Mr and Mrs S, and I recognise that they have been victims of a cruel and manipulative scam. But I don't consider that it would be fair to hold Barclays responsible for their loss, so I won't be asking it to refund that loss to them.

### **My final decision**

I do not uphold Mr and Mrs S' complaint against Barclays Bank UK PLC.

Under the rules of the Financial Ombudsman Service, I'm required to ask Mrs S and Mr S to accept or reject my decision before 5 March 2026.

Rebecca Norris

**Ombudsman**