

DRN-5793444



The complaint

Mr B complains that Barclays Bank UK PLC ('Barclays') declined to refund him £5,250 which he lost as a result of a scam.

What happened

In August 2025, I wrote to both parties to outline my initial thoughts on this dispute. The following is an extract from my provisional decision:

"The details of this complaint are well known to both parties, so I will not go into every detail of what happened here. But, in summary, in April 2024 Mr B was persuaded to send two payments totalling £5,250 to help him access funds he had previously lost as a result of a scam.

Mr B had fallen victim to an investment scam a number of years before, which saw him send money to cryptocurrency which he did not get back. In April 2024, someone called him and said that they were aware of the scam and that the frozen cryptocurrency had been located. They told Mr B that the £9,000 he had invested was now worth around £36,000 and that they could help him access the frozen wallet if he deposited funds for the 'security capital', which would be refunded to him with his returns. Mr B was told the full balance would then be released to him. Mr B was sent screenshots of his funds, and after speaking with the person for some time was persuaded that this was legitimate. He sent £2,650 from his Barclays account via open banking. The person he was speaking to said this had been received, but explained he'd need to send a further payment. So, Mr B sent a further payment of £2,600, again via open banking. He was then told that the withdrawal request was being reviewed, and he would have to pay another sum of money. At this point, Mr B realised he had fallen victim to a scam.

Mr B got in touch with Barclays who looked into what had happened. Barclays declined to refund Mr B's losses. They said that the payments were not so unusual or out of character for his account that they would have indicated that Mr B was at risk of fraud or financial harm. So, they said that they did not need to provide effective warnings or intervene with the payments, and as such had not acted incorrectly in processing the payments. They said that Mr B had been negligent and failed to conduct due diligence and relevant checks. They pointed to the fact that Mr B had fallen victim to the previous investment scam, but still sent funds when he was contacted out of the blue from an unverified or validated mobile number and then continued communication with them over Whatsapp. They also said it was too good to be true that his lost funds had now grown to around £36,000. They argued that this situation should have provided him cause for concern and led him to attempt to conduct some research or checks to ensure it was genuine, and failing to do so meant he had not met the requisite level of care required.

Mr B was not happy with the response from Barclays, so he escalated his concerns to our service. One of our investigators looked into what had happened, and did not recommend that Mr B's complaint be upheld. In summary, this was because they agreed that there was nothing so unusual or out of character about the payments that Barclays ought to have intervened rather than processing the payments. They also said that there was nothing more that Barclays could have done to recover the funds.

Mr B remained dissatisfied and asked that his complaint be reconsidered. As no agreement could be reached, the case has been passed to me to decide.

What I've provisionally 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. If nothing changes, my final decision would likely be as follows.

In broad terms, the stating position in law is that a bank is expected to process payments and withdrawals that a customer authorises, in accordance with the Payment Service 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.

When thinking about what is fair and reasonable in this case, I have considered whether Barclays should reimburse some or all of the money Mr B lost in line with the provisions of the CRM Code it has agreed to adhere to and whether it ought to have done more to protect Mr M from the possibility of financial harm from fraud.

The CRM Code

Barclays is a signatory of the Lending Standards Board Contingent Reimbursement Model ('CRM') Code. The CRM code requires firms to reimburse customers who have been the victims of APP scams like this in all but a limited number of circumstances. It sets out standards that banks, such as Barclays, are expected to meet in terms of protecting their customers from financial harm. But it also sets out expectations that a customer should meet, too. As a starting point, a customer should receive a full refund if they fall victim to an authorised push payment scam such as this one.

In our investigator's view of the complaint, as well as in the correspondence from Mr B's representatives the CRM code was mentioned. This may have been due to the fact the payments were made via open banking. However, we do consider open banking payments to be pushed payments and so I have considered Mr B's case under the CRM here.

There appears to be no dispute that Mr B was the victim of an authorised push payment scam. He thought he was sending money in order to recover money he had lost, and further earnings, but instead it went to a scammer. But Mr B would not be entitled to a full refund if Barclays can fairly and reasonably demonstrate, as they have asserted, that Mr B has failed to meet the requisite level of care under one of more of the listed exceptions set out in the CRM Code.

Those exceptions are:

- 1. The customer ignored an effective warning in relation to the payment being made;*
- 2. The customer made the payment without a reasonable basis for believing that: the payee was the person the customer was expecting to pay; the payment was for genuine goods or services; and/or the person or business with whom they transacted was legitimate.*

**There are further exceptions within the CRM Code, but they do not apply in this case.*

There are also some circumstances in which I would expect Barclays to intervene with payments, which are separate to the CRM code. In accordance with the law, regulators rules and guidance, relevant codes of practice and what I consider to have been good industry practice at the time, I also think Barclays should fairly and reasonably:

- Have been monitoring accounts and any payments made or received to counter various risks, including anti-money laundering, countering the financing of terrorism, and 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 banks are generally more familiar with than the average customer.

- In some circumstances, irrespective of the payment channel used, have taken additional steps, or make additional checks, before processing a payment, or in some cases declined to make a payment altogether, to help protect customers from the possibility of financial harm from fraud.*

This means that there are circumstances where a bank should fairly and reasonably take additional steps or make additional checks before processing a payment, or in some cases decline to make a payment altogether, to help protect customers from the possibility of financial harm.

Did Barclays need to intervene with the payments, by giving Mr B an effective warning or otherwise?

Mr B, via his previous representatives, argued that the payments were unusual and out of character for Mr B's account such that Barclays ought to have intervened or provided an effective warning. He said in summary that:

- The payments went to a cryptocurrency platform and it is well known in the banking sector that scams are often perpetrated through such platforms.*
- He hadn't made payments to cryptocurrency from his Barclays account before. The payments went to a new payee and were relatively high in value. The previous payments from his account which exceeded this amount had gone to regular payees including his own other bank account, his own company or his credit card account.*
- There were two payments sent on the same day to a new payee.*

I do appreciate that the payments were not for inconsequential amounts of money. Over the two payments which took place in one day, Mr B sent £5,250. However, taking into account Mr B's previous account history, I do not think that Barclays ought to have recognised either payment as unusual or out of character for his account such that they would be required to give Mr B an effective warning or otherwise intervene with the payments. I say this because Mr B made genuine payments for larger amounts of money – including payments of £2,500, £3,000 and £5,000 – prior to the scam transactions taking place. He'd also sent two large transactions of £3,000 and £1,000 to the one legitimate payee on the same day previously, so sending two payments to the same payee in one day was not unusual on his account. There was also activity in which Mr B sent four payments of over £1,000 each totalling over £10,000 in one day in his account history. I do appreciate the funds were going to cryptocurrency and a new payee, but this in and of itself would not have been enough to have warranted intervention here. So, when considering all of this, I don't think there was anything so unusual about the payments Mr B made as the result of this scam that should have alerted Barclays to the risk that Mr B was falling victim to a scam. And so it follows, that I do not think that Barclays needed to provide an effective warning or otherwise intervened.

Did Mr B have a reasonable basis for believing that the person he was sending the funds to was legitimate?

I've also considered whether I think Mr B did sufficient due diligence to assure himself that he was paying a legitimate person or company, and I am afraid to say I don't think he did. I say this because he received a call out of the blue about funds he had sent as a result of a scam about four years prior. Whilst they were able to show his loss and screenshots of a wallet that purported to contain his lost funds and a sizeable return on top of this, there was nothing to say he was talking to a legitimate business. It does not appear Mr B did any checks on the person or company he thought he was talking to in order to ensure that they were genuine. I think that the promise of not only him getting his lost funds back, but the sizeable returns too, ought to have seemed too good to be true. When considering all of this,

I think Mr B should have recognised that he needed to do further checks before sending money to someone who had cold-called him and spoken to him over Whatsapp.

I do appreciate that the correspondence sounded professional, and the screenshots looked persuasive, but setting this against everything else I still believe Mr B ought to have recognised he the need for more checks.

So, considering all of this, I don't think Mr B had a reasonable basis for belief here. And so, I think that the exception to the presumption of reimbursement applies here, and so Barclays acted fairly and reasonably by not refunding Mr B under the CRM code.

My provisional decision

If nothing changes, I will not be upholding this complaint."

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.

Barclays responded to my provisional decision to say that they had nothing further to add. Mr B did not respond to my provisional decision. So, for the reasons I outlined in my provisional decision, I do not uphold this complaint.

My final decision

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 30 September 2025.

Katherine Jones
Ombudsman