

## The complaint

Mr A complains that Barclays Bank UK PLC won't refund the money he lost when he was scammed and blackmailed.

## What happened

Mr A has provided Barclays and our service with limited information on events and the dialogue he had with the scammers.

The following appears to be a summary of events which involve a romance / investment scam and blackmail.

- In late April 2025, Mr A met Person N (a scammer) on a dating app and this developed into an online romance.
- Person N told Mr A about her crypto investment hobby and persuaded him to invest in crypto via crypto Company T.
- Mr A trusted Person N and having given his identity details to her, she opened an account / wallet in his name with Company T.
- Mr A and Person N both had access to the wallet, but Person N traded in crypto for him.
- Mr A paid the following three amounts, totalling £2,600, from his Barclays account to his Company T account:
  1. £100 on 2 May 2025.
  2. £1,500 on 3 May 2025.
  3. £1,000 on 3 May 2025.
- Unbeknown to Mr A, his money was stolen from his Company T account by Person N.
- It's unclear whether it was before or after any of the above three payments but, at an unknown point in time, Person N or other scammers used different tactics to get Mr A to pay money from his crypto wallet (which could include these three amounts) so they could steal it. Also, to pay money from his bank accounts.
- It's also unclear when Mr A realised Person N was a scammer.
- The circumstances and timings are unclear, but their tactics appear to be Person N or other scammers:
  - Telling Mr A that the life of Person N's father was at risk.
  - Threatening to share pictures of Mr A (that Person N or the scammers had received / made) and / or reporting him.
- Mr A made a report to the police and contacted Barclays.

Mr A sought a refund from Barclays as he considers that their interventions should've picked up on red flags to uncover the scam. However, Barclays rejected his claim as he made crypto payments via another account in his name.

Mr A brought his complaint to our service. This also included Barclays unfairly dismissing his complaint and being unhelpful. However, our investigator couldn't see that Barclays had done anything wrong.

Mr A disagrees and points out:

- Due to emotional manipulation, deception, and blackmail tactics from the scammers, his judgment was impaired, and he was especially vulnerable leading to inaccurate statements.
- On an intervention call he referenced catfish and scam programmes, which should have signalled emotional vulnerability and potential romance fraud.

As Mr A remains dissatisfied his complaint has been passed to me to look at.

### **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, my decision is not to uphold this complaint and I'll explain why.

I should first say that:

- I'm very sorry to hear that Mr A has been the victim of this cruel and traumatic scam and I genuinely empathise with the impact this has had on him.
- Although I've read and considered everything Mr A has said, I won't be responding to every point individually. If I don't comment on any specific point, it's not because I've not considered it but because I don't think I need to comment on it in order to reach the right outcome.
- Although the voluntary CRM code was in place in 2024, and Barclays signed up to it, as the payments were made to an account in Mr A's own name unfortunately the payments Mr A made aren't covered.
- Regarding recovery, as the payment went to Company T and then to a scammer who emptied the account, I don't think Barclays could've been expected to recover his funds.
- The Payment Services Regulations 2017 (PSR) and Consumer Duty 2023 apply here.

#### **PSR**

Under the PSR 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 Mr A made the payment here, so it is considered authorised.

However, 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.

Banks do have to strike a balance between the extent to which they intervene in

payments to try and prevent fraud and/or financial harm, against the risk of unnecessarily inconveniencing or delaying legitimate transactions.

So, I consider Barclays should fairly and reasonably:

- Have been monitoring accounts and any payments made or received to counter various risks such as anti-money laundering and preventing fraud and scams.
- Have systems in place to look 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 made 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.

#### Consumer Duty

Also, from July 2023 Barclays had to comply with the Financial Conduct Authority's (FCA's) Consumer Duty which required financial services firms to act to deliver good outcomes for their customers. Whilst the Consumer Duty does not mean that customers will always be protected from bad outcomes, Barclays was required to act to avoid foreseeable harm by, for example, operating adequate systems to detect and prevent fraud. Also, recognise signs of vulnerability.

I wouldn't ordinarily expect a bank to put in place human interventions on payments 1 to 3. This is because the three payments were for relatively low amounts, there wasn't a suspicious pattern, crypto payments are legal and common, the daily expenditure wasn't significantly different, banks process thousands of payments each day and as mentioned above must strike a balance when deciding to intervene.

However, Barclays did take steps to protect Mr A, identifying payments that could possibly be a risk, probably because their system identified them as crypto related and unusual transactions for Mr A to make. Also, they would've known crypto payments were volatile and had an elevated risk of being fraud and scams.

Barclays blocked an attempted payment on 1 May 2025, and then put in place a human intervention prior to payment 1. They also put in place human interventions before releasing the other payments.

I looked at the call transcripts and listened carefully to the call recordings to check the effectiveness, consider warnings, relevant educational information and probing to try and detect whether Mr A was at risk of fraud or a scam.

Mr A has only provided minimal information on his dialogue with Person N, so it isn't possible to know whether he was coached on what to say if Barclays intervened. He has though explained that he trusted Person N and, because he was manipulated and under her spell, his judgment was affected, and he chose to give Barclays fraud and scam agents incorrect answers.

Bank agents though are aware that scammers tell customers to lie to them. So, to uncover and detect a scam they're trained to ask questions about the payment to identify possible scam types, give educational information and then probe to detect any scam or fraud.

All the agents identified the payments were going to Mr A's crypto account and Mr A didn't try to hide this.

#### Intervention 1 – prior to the release of payment 1

I consider the first intervention to have been effective considering Mr A had been looking to make a small initial payment and said he would reduce it following the agent's advice to check he could make a withdrawal. Also, the agent probed to find out the type of crypto coin he was investing in, how he knew about it, who set up the account, if he was acting alone, whether he had any crypto experience and asked about his research. Also, she warned him about the risks, made some basic enquiries and gave some educational information on crypto scams relevant to the transaction Mr A communicated.

I found that when giving the agent false answers Mr A was very friendly, sounded very relaxed and confident and all his answers (about how he was acting alone and trialling crypto having done his own research) to be plausible and I don't think there was anything in either his answers or communications for the agent to suspect he wasn't telling her the truth or something was seriously amiss.

#### Intervention 2 – prior to the release of payment 2

Mr A started the call appearing to be trying to pre-empt questions by saying the following, in what I consider to have been a very convincing way:

- *'It's another crypto (payment). It's a crypto account that I have, no one's not telling me to do it. I'm doing this completely by myself. I've done it before. I've researched it'.*
- *'I profit from it. And, uh, III I don't want to stay poor and like, it's a really good way of me earning money. And that's why I need the funds released'.*
- He would *'really hate it if someone was telling me to do something and try to steal my money. So, I'm really cautious'*.
- *'I really really feel bad for all the (scam) documentaries I've seen people have'*.
- *'You just have to be so, so cautious. I'm like, the most cautious person you'll find. So what I'm doing must be pretty good, because I've just literally what I'm doing right now is as stable as it comes, so I'm just being as cautious as I can'*.
- *'You sort of learn how to do, like, real minimum, like, sort of deals and trades and stuff, like you get the hang of it and you can make a really small amount. It's not much, but it's enough'*.
- *'You can make, like, a few quid like you can make 20 30 40 quid here and there it is possible'*.

Despite him covering a number of their intended questions, the agent probed about the investment, the account and whether there was anyone involved such as a broker. However, Mr A confidently gave the same false answers that he gave the first agent. Also, further to his previous mention of withdrawals (to ensure it wasn't a scam) he said he was able to make withdrawals.

The call then moved to educational information, and I found this to be comprehensive. Also, it importantly included the following information that was directly relevant to the scam:

- Scammers request identity documents so they could open an account in your name.
- You should never let anyone make an account for you.
- If you have a personal relationship with someone, you should know who they are.
- Scammers will provide you with the details for your crypto wallet to then log into so it will be compromised from the beginning.

Importantly here, a reason for the educational information being so comprehensive was because Mr A enthusiastically engaged in the conversation. And from the way he engaged, including comments about catfish scams, together with him making comments about his cautiousness and him sounding very assured when giving false but plausible answers to

probing questions, I'm not persuaded he would've given any signals that he was in fact the victim of such a scam. Also, I don't think there was anything in either his answers, tone or pitch for the agent to suspect he was being untruthful, or something was seriously amiss.

### Intervention 3 – prior to the release of payment 3

I found that the third call wasn't as effective as the previous two, because the agent mainly asked closed questions and didn't ask questions about, for example, the type of coin or ability to withdraw. Also, the warnings the agent gave were very brief and delivered very quickly. However, he twice mentioned the importance of giving truthful answers and asked Mr A if anyone was telling him to answer the questions. Despite this Mr A consistently and persuasively made a point of telling him that he was acted alone. Also, that he'd been trading in crypto for nine years and was making small investments. In addition, when the agent suggested he look at crypto scam warnings Mr A commented on that being a good idea.

Although I think this intervention could've been better, even if the agent had asked more probing questions, I think Mr A would've given the same answers that he'd given the other agents who were more thorough. And again, I found that Mr A sounded very assured and I don't think there were any signs for the agent to pick up on that he was vulnerable, and something was amiss.

So, having carefully considered the three interventions that Barclays put in place to try and protect Mr A from financial harm, which I think were effective when combined, due to the plausible answers that Mr A gave and the assured way he communicated with the agents, I don't think it would be fair or reasonable to have expected them to have detected that Mr A was being subjected to a scam and blackmail (if that had occurred on these dates) and prevented the payments being made.

Regarding Mr A's points that his crypto trading experience comment should've been seen as suspicious, as crypto investments are legal and common and customers may have transferred funds from other bank accounts to other crypto providers, I wouldn't have expected this to have raised a concern.

Regarding Mr A's points that the payment amounts were abnormal and for unusually high amounts, although they were higher than normal, I don't think the amounts were significantly high. Also, Barclays did put interventions in place, probably triggered by the high-risk crypto payments, to scrutinise what he was doing.

Regarding Mr A's frustration and loss of time trying to log a scam investigation and claim, I think Barclays apology and £50 payment is a fair and reasonable resolution. This is because Mr A initially said he was coerced and blackmailed into making the payments and later said it was a romance scam. Also, I think it was difficult for Barclays agents to understand the events that had occurred, and they treated Mr A sympathetically and looked to support him.

Having considered the above and all the information on file, whilst I'm genuinely very sorry that Mr A has lost this money and had such a traumatic experience, I don't think Barclays missed opportunities to uncover the scam or treated Mr A unfairly. So, I'm not upholding this complaint and requiring Barclays to make a refund.

## **My final decision**

For the reasons mentioned above, my final decision is that I'm not upholding this complaint against Barclays Bank UK PLC.

Under the rules of the Financial Ombudsman Service, I'm required to ask Mr A to accept or reject my decision before 19 December 2025.

Paul Douglas  
**Ombudsman**