

## The complaint

Mr S complains that HSBC UK Bank Plc ('HSBC') won't refund the money he lost after falling victim to a scam.

## What happened

In 2024, Mr S met someone through a dating site, who introduced him to cryptocurrency trading.

Mr S made payments from his HSBC account to purchase cryptocurrency, which was sent to wallets controlled by the scammer.

Initially Mr S made payments as part of the investment scam, believing that he was buying and selling cryptocurrency through a company I'll refer to as B. When Mr S tried to withdraw the profits he'd earned from B, he was told he had to make payments due to anti-money laundering issues. Having made the payments, Mr S still wasn't able to withdraw his funds from B. Mr S was then contacted by someone who said they could help him recover his funds if he made additional payments.

Unfortunately, all of the individuals that Mr S dealt with were scammers, and he lost all of the money he sent from his HSBC account.

These are the payments Mr S made from his HSBC account as part of the scams.

Date	Pmt	Details of transaction	Amount
25.9.2024	1	Payment to C – a cryptocurrency exchange	£383.66
25.9.2024	2	Payment to C – a cryptocurrency exchange	£2,000.00
28.9.2024	3	Payment to C – a cryptocurrency exchange	£100.00
28.9.2024	4	Payment to C – a cryptocurrency exchange	£1,400.00
29.9.2024	5	Payment to C – a cryptocurrency exchange	£3,765.00
10.10.2024	6	Payment to C – a cryptocurrency exchange	£2,951.08
16.10.2024	7	Payment to C – a cryptocurrency exchange	£40.00
16.10.2024	8	Payment to C – a cryptocurrency exchange	£10.00
17.10.2024	9	Payment to C – a cryptocurrency exchange	£50.00
17.10.2024	10	Payment to C – a cryptocurrency exchange	£45.00
17.10.2024	11	Payment to C – a cryptocurrency exchange	£8.00
18.10.2024	12	Payment to C – a cryptocurrency exchange	£48.00
22.10.2024	13	Payment to C – a cryptocurrency exchange	£560.00
31.10.2024	14	Payment to C – a cryptocurrency exchange	£387.00
2.11.2024	15	Payment to C – a cryptocurrency exchange	£80.00
2.11.2024	16	Payment to C – a cryptocurrency exchange	£275.00
3.11.2024	17	Payment to C – a cryptocurrency exchange	£275.00
3.11.2024	18	Payment to C – a cryptocurrency exchange	£20.00.
3.11.2024	19	Payment to C – a cryptocurrency exchange	£405.00
4.11.2024	20	Payment to C – a cryptocurrency exchange	£647.00
5.11.2024	21	Payment to C – a cryptocurrency exchange	£100.00

29.11.2024	22	Payment to C – a cryptocurrency exchange	£320.00
4.12.2024	23	Payment to C – a cryptocurrency exchange	£1,000.00
5.12.2024	24	Payment to C – a cryptocurrency exchange	£1,303.56
5.12.2024	25	Payment to C – a cryptocurrency exchange	£50.00

Mr S reported the scam to HSBC through a professional representative. HSBC declined to refund Mr S saying his payments aren't covered by the Contingent Reimbursement Model Code (CRM Code) or the Payment Service Regulator's APP Scam Reimbursement Rules – as neither scheme covers payments made to an account in the customer's own name. Also, HSBC didn't consider they'd made an error when the payments were made, as they intervened on 28 and 29 September and asked Mr S the reason for the payments. HSBC say Mr S was shown onscreen warnings related to the payment purpose he selected – that he was paying himself.

Mr S wasn't happy with HSBC's response, so he brought a complaint to our service.

An investigator looked into Mr S's complaint but didn't uphold it. The investigator wasn't satisfied that HSBC were required to intervene when the payments were made, saying they weren't unusual or out of character for his account.

Mr S's representative disagreed with the investigator's opinion and raised the following points:

- Mr S doesn't recall seeing any onscreen warning/s when he made the payments.
- HSBC's intervention wasn't sufficient in light of the repeated payments to cryptocurrency by a novice customer. Also, Mr S making payments in excess of £16,000 between September and December was out of character for his account.
- There should've been further intervention by HSBC including dynamic friction warnings, real-time blocking and education regarding cryptocurrency investment scams and release fee scams.

The investigator responded to the points raised saying that the payments weren't identifiably related to cryptocurrency as they went to a payment service provider who doesn't solely deal in cryptocurrency accounts. And the warnings that HSBC provided were proportionate to the risk identified, with the warning tailored to the payment purpose Mr S selected.

Mr S still disagreed and asked for an ombudsman to review his case.

Having reviewed the case, I reached the same answer as the investigator but for slightly different reasons. So, I issued a provisional decision explaining why and giving both parties a chance to respond before a final decision was issued.

### **My provisional decision**

In my provisional decision section "What I've decided – and why" I said:

I've considered all the available evidence and arguments to decide what's fair and reasonable in the circumstances of this complaint.

In deciding what's fair and reasonable, I am required to take into account relevant law and regulations, regulators' rules, guidance and standards, and codes of practice; and, where appropriate, I must also take into account what I consider to have been good industry practice at the time.

In broad terms, the starting position at law is that a bank is 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. It's not in dispute that Mr S authorised these payments, although he did so not realising he was the victim of a scam.

### HSBC's intervention

HSBC intervened on 28 and 29 September and asked Mr S the reason for the payments. Mr S said he was paying the money to himself, so HSBC provided an onscreen warning related to safe account scams. This is what the warning said:

#### ***Could this be fraud?***

*You could lose your money*

#### ***Is this:***

*A new account?*

*Did someone else:*

*Open it for you?*

*Is someone asking you to send money to a 'safe account'?*

*If someone has told you to mislead us about the payment reason or asked you to send money to a 'safe account', this is fraud. Stop now.*

*If you're making an investment or buying cryptocurrency, you've chosen the wrong payment reason. Please go back and choose the right one. If you have any doubts, stop the payment.*

I would've expected HSBC to have intervened when Mr S made payment five on 29 September. I say this taking into account the size of the payment and because I think it's more likely than not the payment was identifiably related to cryptocurrency based on the sort code that Mr S used for the payee, which was linked to C – a cryptocurrency exchange.

As a result, I would've expected HSBC to have provided Mr S with an onscreen warning tailored to cryptocurrency investment scams. This should've highlighted the key features of these scams including being endorsed by high-profile individuals, returns that are too good to be true, being advertised on social media sites, and returns being guaranteed (as these investments usually involve a level of risk).

However, I'm not satisfied that an onscreen warning of this type would've resonated with Mr S or prevented him from making his payment. I'll explain why.

Mr S hadn't found the investment on social media, and it wasn't endorsed by a high-profile individual. It was introduced to him by someone he had met through a dating site and spent weeks talking to. The scammer had told Mr S that he could expect a return of 10-15% on his capital, which was too good to be true. But the scammer had also built up a rapport with Mr S and it's clear that he was invested in the relationship they had built by the time he made payment five.

So, even if HSBC had provided a cryptocurrency investment scam warning onscreen, I'm not satisfied it would have prevented Mr S's loss from payment five.

### Should HSBC have intervened again?

While I appreciate that all of the payments were made to the same payee, and the funds were going to an account in Mr S's own name, I still would've expected HSBC to have intervened again after payment five. I say this taking into account that the payments were identifiably related to cryptocurrency, the heightened risk associated with cryptocurrency payments and the ongoing payments that Mr S made to C.

I would've expected the next intervention to have been a call to Mr S to discuss the payments. But I'm not persuaded that a call to Mr S would've prevented any further payments.

Mr S was talking to the scammer multiple times per day – often talking from first thing in the morning until last thing at night, and they were sharing all aspects of their lives with each other. They were discussing their families and their future plans and it's clear that Mr S was under the scammer's spell. Unfortunately, romance scams are designed to get the victim hooked emotionally through “love bombing” and the belief that they are involved in a genuine relationship which has the prospect of becoming serious. By building the personal relationship, the scammer was able to take advantage of Mr S's feelings for her and pressure him into doing things that he might not otherwise have normally done.

So, if HSBC had called Mr S and explained why they thought he was the victim of an investment scam, I'm not satisfied I can fairly say it's more likely than not that Mr S would've believed HSBC over the scammer. It's possible that it would've given him pause for thought, but I think he would most likely have messaged the scammer and they would've given him multiple reasons why it wasn't a scam – which Mr S would've believed.

I realise that I'm making a conclusion on what I think Mr S's actions would've been in a hypothetical situation. However, I only have to reach a decision on the balance of probabilities. In other words, what I think would more likely than not have happened based on the available evidence.

In this case, I'm not convinced that HSBC talking to Mr S about the payments would've broken the spell the scammer had him under or meant that he wouldn't have continued with making payments.

I'm really sorry that Mr S was the victim of a very cruel scam which involved emotional manipulation and coercion. I realise that he has suffered a serious financial loss including taking out loans to fund the payments, which he can't afford to repay.

But having carefully considered all of the evidence, I'm not satisfied that I can fairly hold HSBC liable for his loss.

My provisional decision was that I didn't intend to uphold this complaint.

### **Responses to my provisional decision**

HSBC responded to say they didn't have anything further to add.

Mr S responded to say he disagreed with the provisional decision for the following reasons:

- There should've been more intrusive and proportionate intervention earlier and, on this basis, there should be a partial uphold.

- It's speculative to say that further questions or warnings wouldn't have broken the scam's momentum and prevented Mr S's loss.
- The evidential threshold used was too high.
- There are procedural concerns about a lack of full case-specific analysis and limited engagement with submissions.

### **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'd like to reassure Mr S that I have considered all of the facts, testimony and evidence provided in reaching my answer on his case. Where there is a lack of information or evidence, for example, where I believe HSBC should've intervened but didn't, I only have to reach a decision based on the balance of probabilities.

The fact that HSBC didn't intervene when I think it should've doesn't mean that Mr S is entitled to a partial refund. I have to consider what I think would more likely than not have happened as a result of that intervention and whether I'm satisfied that it would've prevented Mr S's loss.

I'm still satisfied that HSBC should've intervened on 29 September 2024 and provided an onscreen warning related to cryptocurrency investment scams. I wouldn't have expected HSBC to have intervened prior to this point, taking into account the size and pattern of the payments.

But I'm not satisfied that an onscreen warning would've resonated with Mr S and the circumstances under which he found the investment. So, I'm not persuaded an onscreen warning would've prevented Mr S's loss.

I would've expected HSBC to have intervened again after payment five, but I'm still not persuaded that this further intervention would've prevented Mr S from making payments.

I say this based on the messages between Mr S and the scammer. I can see they had developed a relationship, and the scammer had built a level of trust with him. They were constantly communicating throughout each day and discussing future plans.

So, even if HSBC had asked about the purpose of the payments or provided a relevant warning, I think it's more likely than not that the scammer would've reassured Mr S that they were genuine and that Mr S would've put more trust in what the scammer told him than what HSBC said. In this case, Mr S wasn't just the victim of an investment scam but also a romance scam, which meant the scammer used emotional manipulation in getting Mr S to make the payments.

I'm really sorry that Mr S has lost these funds and been the victim of a cruel scam. But, having considered all of the evidence, I'm not satisfied that I can fairly hold HSBC liable for his loss.

### **My final decision**

My final decision is that I don't uphold this complaint against HSBC UK Bank Plc.

Under the rules of the Financial Ombudsman Service, I'm required to ask Mr S to accept or reject my decision before 17 February 2026.

Lisa Lowe  
**Ombudsman**