

The complaint

Mr S complains that HSBC UK Bank Plc ('HSBC') hasn't refunded the money he lost to a cryptocurrency investment scam.

What happened

The circumstances of the complaint are well-known to both parties. So, I don't intend to set these out in detail here. However, I'll provide a brief summary of what's happened.

In November 2021, Mr S made two payments, totalling £32,350, from his HSBC account to his digital wallet with a cryptocurrency exchange platform – which I'll refer to as 'K'. The funds were converted into cryptocurrency and sent to a third party – which I'll refer to as 'H'.

Mr S thought H was a genuine business, helping customers to invest in cryptocurrency. However, it later came to light that H was a scam and Mr S had lost the money he invested.

After realising he'd been the victim of a scam, Mr S reported the situation to HSBC in the form of a complaint. In response to the complaint, HSBC said it wasn't responsible for refunding Mr S's loss, as it thought the situation was a civil dispute between Mr S and H, and that it hadn't done anything wrong in approving Mr S's payments.

Unhappy with HSBC's response, Mr S referred his complaint to this service. Our Investigator considered the complaint but didn't uphold it. Whilst they thought Mr S had been the victim of a scam, they didn't think the scam payments were unusual or suspicious at the time they were made, meaning HSBC couldn't reasonably have been expected to have intervened and questioned Mr S about them before approving them.

Mr S didn't agree. He said that there was an apparent scam risk when the payments were made and that HSBC ought to have done more to verify that the payments were being made for a genuine reason *before* approving them. If that had happened, the scam could've been prevented.

As an agreement couldn't be reached, the complaint has been passed to me to decide.

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.

In deciding what's fair and reasonable in all the circumstances of a complaint, I'm required to take into account relevant: law and regulations; regulators' rules, guidance and standards; codes of practice; and, where appropriate, what I consider to have been good industry practice at the time.

In their view, our Investigator set out, in detail, why they thought H was most likely a scam and not a civil dispute as HSBC had argued. HSBC didn't provide a response to whether H should be treated as a scam or not. So, for simplicity – and as it wouldn't change the outcome of the complaint – my decision has focused on whether HSBC reasonably could've prevented Mr S's loss and if it can fairly be held responsible for reimbursing Mr S.

At the time Mr S made the disputed payments, HSBC was signed up to the Lending Standards Board's Contingent Reimbursement Model Code ('the CRM Code'). The CRM Code provides additional protection from authorised push payment ('APP') scams, but only in certain circumstances. For example, the CRM Code doesn't apply to payments made by a customer to their own account with a different provider.

In this case, Mr S made the scam payments to his own digital wallet with K, which he had full control over and was able to use the funds to purchase cryptocurrency, which he sent to H. As Mr S sent funds from HSBC to his own digital wallet with K, I'm satisfied that the CRM Code doesn't apply in his circumstances and it's not a relevant consideration in this complaint.

However, that isn't the end of the story. Good industry practice required HSBC to be on the lookout for account activity or payments that were unusual or out of character to the extent that they might indicate a fraud risk. On spotting such a payment, I'd expect it to take steps to warn the customer about the risks of proceeding.

Our Investigator didn't think the scam payments were so unusual that HSBC reasonably ought to have been concerned by them. Mr S says the scam payments did demonstrate an APP scam risk to HSBC at the time they were made, although he hasn't explained why he thinks this. So, I've carefully considered whether I think the scam payments demonstrated an APP scam risk to HSBC.

The scam payments were both for large amounts – £18,650 on 6 November 2021; and £13,700 a week later. They were also going to a cryptocurrency exchange platform. So, on the face of it, I can understand why Mr S thinks HSBC should've been concerned by the payments, given the amounts and the destination of his funds.

However, I'm not persuaded HSBC reasonably ought to have been concerned by the scam payments to the extent that I would've expected it to have intervened and questioned Mr S about them. I don't think HSBC missed an opportunity to identify the scam and prevent the funds being sent. As a result, I don't think HSBC can fairly be held responsible for Mr S's loss. I know this outcome will disappoint Mr S, so I'll explain why.

HSBC has provided Mr S's bank statements from August 2020 until November 2021. I've carefully reviewed these to understand Mr S's typical payments activity. During this period, Mr S had a high account turnover. He regularly paid large amounts into the account, which were quickly moved on to other accounts, usually in his own name. This same pattern took place when he made the scam payments to K. So, there wasn't anything unusual about Mr S moving money into the account and quickly moving these funds on to another account in his own name, as he had been regularly doing this for at least 15 months.

Prior to the first scam payment, Mr S had made 11 payments for higher payment values than £18,650. He'd also made 16 payments (not including the first scam payment) for higher values than the £13,700 payment. There were also eight other payments of around £10,000 or more, which didn't exceed the value of the scam payments, but were also large in value. So, Mr S was regularly using his HSBC account to make large payments. Whilst the two scam payments were for large amounts, they weren't so large that they appeared unusual or out of character for Mr S.

Mr S had opened an account with K around a month before the scam payments were made and had already made five payments from his HSBC account. He'd also made a withdrawal from K into his HSBC account. Whilst the scam payments were larger than the initial payments to K, by the time the scam payments were made, K was an established beneficiary, that he'd already sent over £7,000 to. So, I don't think HSBC reasonably ought to have been concerned that Mr S was sending large amounts to K.

Taking into account Mr S's typical account activity, I'm not persuaded that the scam payments demonstrated an APP scam risk to HSBC at the time Mr S made them. The scam payments appeared consistent with his regular use of the account and the funds were being sent to his own digital wallet which he'd paid several times before.

I appreciate Mr S thinks HSBC would've uncovered the scam and prevented his loss *if* it had spoken to him about the scam payments. However, in the circumstances, I can't agree that HSBC reasonably ought to have questioned Mr S about the payments because they weren't out of character or suspicious. As a result, I don't think HSBC missed an opportunity to prevent the scam payments being made and it can't fairly be held responsible for Mr S's loss.

I'm also not persuaded that HSBC could've done anything to recover Mr S's loss. The funds were sent to his own digital wallet with K, where they were converted into cryptocurrency and sent to H. As Mr S had already utilised the funds and sent them from his digital wallet with K, there was nothing for HSBC to recover.

My final decision

For the reasons explained above, my final decision is that I don't uphold this complaint about 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 6 June 2025.

Liam Davies
Ombudsman