

## **The complaint**

Mr W is complaining that HSBC UK Bank Plc hasn't reimbursed him for payments he says he made to a scam.

## **What happened**

Both parties are familiar with the background to this complaint so I won't go into detail here.

In short, in late 2023 Mr W says he fell victim to a cryptocurrency investment scam.

He made payments to the scam over the course of around two months, between October 2023 and December 2023. Some payments were made directly to a cryptocurrency exchange and some were made to his accounts with other businesses by faster payment (from where they were sent on to the scam.)

When he realised he'd been the victim of a scam, Mr W complained to HSBC. But it didn't uphold his complaint. Unhappy with its response, Mr W referred his complaint to the Financial Ombudsman.

Our Investigator looked into Mr W's complaint, but he didn't think HSBC ought to have done anything to intervene to prevent Mr W from making the payments. Mr W didn't agree, so his complaint has been passed to me for review and a 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.

I'm sorry to disappoint Mr W, but I'm not upholding his complaint - for much the same reasons as the Investigator. I'll explain why.

The evidence Mr W has provided of his involvement in the scam looks to be fairly generic, and I'd usually be looking for some more evidence to show that Mr W was involved in the scam and had suffered a loss because of it. But because this doesn't make a difference to the outcome of Mr W's complaint, I'm going to proceed on the basis that Mr W *did* suffer a loss to the scam he's described.

I've thought about the Contingent Reimbursement Model (CRM) code which can offer a potential means of obtaining a refund following Authorised Push Payment (APP) scams. But the CRM code doesn't apply to payments made by debit card, or to payments made to another account in the customer's own name, so Mr W's payments aren't covered by it. I've therefore considered whether HSBC should reimburse Mr W under any of its other obligations.

It's not in dispute that Mr W authorised the payments. And HSBC had a duty to act on his instructions. But in some circumstances a bank should take a closer look at the circumstances of the payments – for example, if it ought to be alert to a fraud risk, because

the transaction is unusual for the customer, or otherwise looks characteristic of fraud. And if so, it should intervene, for example, by contacting the customer directly, before releasing the payments. But I'd expect any intervention to be proportionate to the circumstances of the payment.

But I've also kept in mind that banks such as HSBC process high volumes of transactions each day. There is a balance for it to find between allowing customers to be able to use their account and questioning transactions to confirm they're legitimate.

When HSBC logged Mr W's scam claim, it seems it only included the payments he made in November 2023. But I note Mr W did mention that he'd made smaller payments directly to the cryptocurrency exchange in the reporting call – and the Investigator has included the payments made to the cryptocurrency exchange in October 2023 and December 2023 in his view, and neither party has questioned this. So, I'll proceed on the basis that the scam payments included the payments made to the cryptocurrency exchange in October 2023 and December 2023.

I have reviewed the available statements which show Mr W's general account activity, along with the payments he made to the scam. And having considered when they were made, their value and who they were made to, I'm not persuaded HSBC ought to have found any of the payments suspicious, such that it ought to have made enquires of Mr W before processing them.

The disputed payments here were made over, broadly, a two-month period, and didn't escalate rapidly in frequency or value, in the way that can sometimes indicate a scam may be taking place.

Some of Mr W's payments were made to a cryptocurrency exchange – but these payments were simply not of a value where I'd expect HSBC to be concerned about Mr W being at risk of financial harm from a scam, because no individual payment was higher than £100. I've taken into account that the payments were made to a cryptocurrency exchange, and at the time the payments were made I'd expect HSBC to have been aware of the increased risk to its customers of multistage fraud, often including payments to cryptocurrency. But that doesn't mean payments to cryptocurrency should automatically be treated as suspicious – people can, and do, make legitimate payments to cryptocurrency.

I've also considered Mr W's other payments, which were made to other accounts held in his name. Some payments were made to two different Electronic Money Institutions (EMI's) and one was made to his account with another bank. The payment of £5 to Mr W's account with another bank, and £500 to Mr W's account with one of the EMI's were, similarly, not of a value where I'd have expected HSBC to have been concerned. However, Mr W did make payments of a greater value to the other EMI. He made four payments to this EMI, ranging in value from £700 to £4,200, and two of the payments – for £4,200 and £1,650 – were made on the same day.

I've thought carefully about whether HSBC should have found these payments to be concerning, such that it ought to have intervened. And taking everything into account, I don't think it should have. While I accept that some of the payments were of greater value than the payments Mr W usually made from this account, it's not unusual for customers to occasionally make higher value payments than they usually do, and this is only one of the factors I'd expect HSBC to have considered when deciding whether to intervene. The payments were being made to an account in Mr W's own name, and although as I've explained HSBC should, at this time, have been aware of the risk of multi-stage fraud such as Mr W was experiencing, I think it could have taken some reassurance from this in these circumstances.

Having considered all the circumstances, I don't think it was unreasonable for HSBC not to view the payments as suspicious, such that it should have carried out any additional checks or given an additional warning before processing the payments. So, I don't think HSBC ought to have done any more to prevent the payments Mr W made.

I've also thought about whether HSBC could have done more to recover Mr W's funds once the scam had been reported. But here, the payments made by faster payment were made to other accounts in Mr W's name, before being sent on to the scam. So, it's difficult to see how recovery would have been possible in these circumstances. It looks like some of the payments to the cryptocurrency exchange were made by debit card, but any chargeback claim raised would likely have been unsuccessful, because the cryptocurrency exchange provided the service Mr W paid for in providing the cryptocurrency.

I know this outcome will be disappointing for Mr W and I'm sorry for that. But for the reasons I've explained, I don't think HSBC should have done more to prevent his loss. So, it wouldn't be reasonable for me to ask it to refund the payments he made.

### **My final decision**

My final decision is that I'm not upholding Mr W's complaint.

Under the rules of the Financial Ombudsman Service, I'm required to ask Mr W to accept or reject my decision before 21 April 2025.

Helen Sutcliffe  
**Ombudsman**