

Complaint

Mr C is unhappy that HSBC UK Bank Plc didn't reimburse him after he reported falling victim to a scam.

Background

In July 2024, Mr C received an unsolicited phone call from someone who said they had discovered an e-wallet containing the proceeds of a cryptocurrency investment Mr C had made some years ago. They said they represented a firm that could help him with recovering his investment. However, he was told he'd need to pay administrative fees and taxes to do so. Unfortunately, Mr C didn't realise it at the time, but he wasn't speaking to a genuine financial services firm, but a fraudster.

The fraudsters guided him through the process of setting up an account with a third-party business. They asked him to download remote access software to allow them to help him with this. He deposited funds, via the third-party business, into an account in his own name. Those funds were then converted into cryptocurrency and that cryptocurrency was subsequently transferred into the control of the fraudsters.

He used his HSBC account to make the following payments:

1	10 July 2024	£300
2	10 July 2024	£300
3	12 July 2024	£1,160
4	12 July 2024	£2,000
5	15 July 2024	£2,000
6	16 July 2024	£1,000
7	17 July 2024	£2,000
8	18 July 2024	£1,200

He was told his investment would be returned to him by a particular deadline. When that deadline passed and he didn't get his money back, he realised he must have fallen victim to a scam.

Mr C notified HSBC of the scam. It didn't agree to refund him. It said that, as Mr C had made payments to an account in his own name, he didn't benefit from any of the protections of the Lending Standards Board's Contingent Reimbursement Model Code ("CRM Code"). It also said it had taken reasonable steps to protect Mr C. It had spoken to him on a number of occasions and warned him about the risk of investment scams.

Mr C wasn't happy with the response he received from HSBC and so he referred his complaint to this service. It was looked at by an Investigator who didn't uphold it. Mr C didn't agree with the Investigator's opinion and so the complaint has been passed to me to consider and come to a final decision.

Findings

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

In broad terms, the starting position at law is that a firm is expected to process payments and withdrawals that a customer authorises, 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 common ground that these payments were authorised by Mr C and so he is presumed liable at first instance.

HSBC was a signatory to the CRM Code which requires firms to pay refunds to victims of scams in certain circumstances. However, it doesn't cover all types of payments. The fact that Mr C made payments to an account in his own name means the CRM Code doesn't apply here. However, that isn't the end of the story. Good industry practice required that HSBC 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 protect its customer. That might be as simple as providing a written warning as part of the payment process or it might extend to making contact with the customer to establish the circumstances surrounding the payment.

I can see that HSBC did intervene in connection with several of these payments. Mr C's representatives have made some well-founded criticisms of the way those calls were handled. The employee of the bank didn't sufficiently probe the answers Mr C gave. However, in order for me to uphold his complaint, I need to be persuaded that any error on the part of the firm was a cause of the loss – in other words, if HSBC had handled things as I'd have expected, would it have prevented the loss Mr C went on to suffer?

I've considered that point carefully and I think it's highly unlikely that HSBC could've prevented any of these payments. The way Mr C responded to queries from the bank put it in a difficult position in respect of its efforts to protect him from the risk of fraud.

For example, he told the call handler that he hadn't been asked to download remote access software by anyone. Unfortunately, that was false. If he'd answered that question truthfully, it would've been an unambiguous red flag. When responding to the call handler's questions, he also said that he *"literally just started the investment."* However, Mr C was acting in the belief that he was recovering funds from an earlier investment. Unfortunately, there was an undeniable reticence about answering the bank's questions openly and fully.

I agree with Mr C's representative when it says that banks ought to be heedful of the risk of customers providing partial or misleading answers to questions. It's well known in the industry that fraudsters talk victims through the way they need to respond to questions from the bank so as to circumvent fraud prevention efforts.

The call handler told Mr C that, on occasion, *"fraudsters have coached our customer into not telling the truth when speaking to the bank around the purpose of the payment..."* He said that wasn't the case with him. Mr C's representative told us that he didn't believe he was being coached because he believed he was paying for a legitimate service. However, it's difficult to square that with the fact Mr C also says that, as a result of his conversations with the scammer, he'd come to believe that banks were *"against cryptocurrency payments and would block any attempts."*

Any advice he was given to mislead the bank doesn't appear to be contained in the messages he exchanged with the fraudster. However, it's revealing that the fraudster asks Mr C to contact them if HSBC made contact and, at one point, says, *"if they call you from*

fraud department, you know how to talk to them.” Fundamentally, I think the Mr C had accepted the premise that the banks wouldn’t allow him to make these transactions if he answered its questions truthfully and he’d been coached on how to respond if questioned. Even if the employee of the bank had questioned him further, I find it more likely than not that they wouldn’t have been able to establish Mr C’s real intentions with the payments.

I don’t say any of this to downplay or diminish the fact that Mr C has fallen victim to a cruel and cynical scam. I have a great deal of sympathy for him and the position he’s found himself in. However, my role is to look at the actions and inactions of the bank and, while I agree it ought to have handled things differently here, I am not persuaded that any shortcoming on the its part was a cause of the losses Mr C went on to suffer.

Final decision

For the reasons I’ve explained above, I don’t uphold this complaint.

Under the rules of the Financial Ombudsman Service, I’m required to ask Mr C to accept or reject my decision before 10 December 2025.

James Kimmitt
Ombudsman