

The complaint

Mr G complains that HSBC UK Bank Plc (HSBC) won't refund money he lost in an investment scam.

What happened

What Mr G says:

In March 2023, Mr G met someone on a dating website and they struck up a relationship. They corresponded via WhatsApp.

After a short time, they discussed crypto currency investments and the scammer encouraged Mr G to make some crypto investments. He made the following payments and receipts. The payments were partly funded by a loan:

Date	Payment	Amount
22 March 2023	Bill payment - Crypto wallet	£100
23 March 2023	Bill payment - Crypto wallet	£400
27 March 2023	Loan drawn	(£5,000) - credit
27 March 2023	Bill payment - Crypto wallet	£5,000
28 March 2023	Credit from Crypto wallet	(£5,989.04) - credit
28 March 2023	Loan repaid	£5,000
3 April 2023	Bill payment - Crypto wallet	£4,000
11 April 2023	Loan drawn	(£5,000) - credit
11 April 2023	Bill payment - Crypto wallet	£5,000
13 April 2023	Bill payment - Crypto wallet	£1,500
Total net loss		£10,010.96

Mr G became aware it was a scam when he wanted to withdraw some money and was told he needed to pay more to meet taxes and fees. He says the investment website was a fake. The WhatsApp messages stopped.

Mr G says he lost all his savings, and some of his mother's money – as she helped him with some of the investments. He says he'd fell victim to a clever, multi layered scam. He says

HSBC had a legal and moral duty to protect him but didn't. He says HSBC should refund the money he's lost.

What HSBC said:

HSBC said the payments were made to a crypto wallet in Mr G's name and as such they were made to an account under his control. The Contingent Reimbursement Model (CRM) code didn't apply for that reason.

HSBC said the funds were sent to the investment from the crypto wallet. Mr G should therefore approach the provider of the crypto wallet to ask for a refund.

Our investigation so far:

Mr G brought his complaint to us. Our investigator didn't uphold it. HSBC intervened in the payments for £4,000 (3 April 2023) and £5,000 (11 April 2023) and on the calls, he was satisfied HSBC asked the right questions, and gave sufficient warnings to Mr G.

Mr G didn't agree. He said HSBC's questions only related to the payments to his crypto wallet and didn't address the end investment – to where the funds were then transferred from the wallet. He asked that an ombudsman look at his complaint, and so it has come to me to make a final 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 hear that Mr G has lost money in a cruel scam. It's not in question that he authorised and consented to the payments in this case. So although Mr G didn't intend for the money to go to a scammer, he is presumed to be liable for the loss in the first instance.

So, 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 and the terms and conditions of the customer's account. And I have taken that into account when deciding what is fair and reasonable in this case.

But that is not the end of the story. Taking into account the law, regulators rules and guidance, relevant codes of practice and what I consider to have been good industry practice at the time, I consider HSBC should fairly and reasonably:

- Have been monitoring accounts and any payments made or received to counter various risks, including anti-money laundering, countering the financing of terrorism, and preventing fraud and scams.
- Have had systems in place to look out 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 make 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.

The Lending Standards Board Contingent Reimbursement Model Code (CRM Code) doesn't apply in this case. That is because it applies to faster payments made to another UK

beneficiary– and in this case, the payments were made to Mr G's own account– his crypto wallet.

I need to decide whether HSBC acted fairly and reasonably in its dealings with Mr G when he made the payments, or whether it should have done more than it did. I have considered the position carefully.

If the payments were of a sufficient size and were out of character with how Mr G normally used his account – then we would expect HSBC to have intervened and spoken to Mr G about them. I looked at Mr G's account, and it's fair to say that the payments were unusual compared to the way in which he used his account – which was to receive his salary and make day to day expenditures of relatively low value.

But – on the other hand, there's a balance to be struck: HSBC has obligations to be alert to fraud and scams and to act in their customers' best interests, but they can't be involved in every transaction as this would cause unnecessary disruption to legitimate payments. In this case, I think HSBC acted reasonably in processing the first payments of £100, £400 and then £5,000 on 27 March 2023. This was funded by a loan for the same amount.

Mr G then received a credit for £5,989.04. I can see from the WhatsApp chats with the scammer that this was paid from the 'investment' to his crypto wallet and then transferred to his bank account with HSBC. It represented the repayment of the first 'investments', plus some 'profit'. As Mr G has told us – this was probably a tactic to show him the investment was 'genuine'. I can also see that the scammer introduced Mr G to the fake website (which showed his 'investments' were doing well) and coached him how to transfer money from his crypto wallet to the 'investment' – she provided the web address/link for him to do so.

But equally – HSBC told us that the credit of £5,981 also showed that the transfer beneficiary (i.e. Mr G's crypto wallet) was a genuine one – and their systems recognised it as such.

But when Mr G tried to make further payments for £4,000 (3 April 2023), and then £5,000 (11 April 2023) – they intervened and stopped the payments and spoke to Mr G about them. These were important calls - and I listened to them. I quote parts of the calls:

Call – 3 April 2023 - £4,000:

Overall, Mr G sounded very confident on the call – he said that he wanted to go ahead.

Mr G: *'I had a fraud warning. I want to do it (make the payment). It's a known source'.*

HSBC: Payment for £4,000 held for fraud checks. Has the previous payment (for £5,000) been received into your account? *Mr G: yes.*

HSBC: What is the purpose of the payment? *Mr G: to fund a crypto investment.*

HSBC: You made previous payments of £100 and £400? *Mr G: yes, to ensure all was working properly.*

HSBC: Has anyone told you how to answer our questions or asked you to mislead us in any way? *Mr G: no, not at all.*

HSBC: You drew a loan of £5,000? Was that to invest in crypto? *Mr G: yes.*

HSBC: The credit for £5,981 – are you aware of that? *Mr G: yes.*

HSBC: Was it a trial for the crypto wallet? *Mr G – yes, pretty much, I made money so that's good.*

HSBC: Gave a warning: there are criminals out there using sophisticated methods for investment scams, getting unsuspecting people to hand over money. They can appear knowledgeable and look genuine - using professional looking websites, marketing material, and testimonials. Be careful to check where you are sending your money. If the payment turns out to be fraudulent, we may not be able to refund it. *Mr G: sure.*

HSBC: Have you received any calls, texts, calls asking you to make this payment? *Mr G: no*

HSBC: Based on these questions, do you want more time to consider? *Mr G: no, I'm satisfied and appreciate the diligence of HSBC in monitoring transfers.*

Call – 11 April 2023 - £5,000:

Again, Mr G was confident in his answers and said he wanted to go ahead.

HSBC: This is a fraud check for the payment of £5,000. *Mr G: yes, I've made a number of these before.*

HSBC: Has anyone told you how to answer our questions? *Mr G: no, not at all.*

HSBC: Tell me more about the background to this payment. *Mr G: it's an investment .*

HSBC: Into a Crypto investment? *Mr G: yes, crypto.*

HSBC: Is this going into a scheme offering higher than normal returns? *Mr G: not a scheme as such.*

HSBC: What checks have you done? *Mr G – checked the wallet provider and it's registered/ authorised with the FCA.*

HSBC: Have you got funds back from your wallet? *Mr G: yes, it works both ways.*

HSBC: Will you make further investments? *Mr G: yes.*

HSBC: any contact from third parties asking you to make this payment? *Mr G: no.*

HSBC: then read out the same warning as on the 3 April 2023 call.

HSBC: so – be careful. *Mr G: Absolutely.*

HSBC: Are you making payment to the provider (of the investment)? *Mr G: unsure, I've done it before, it's all trusted and legitimate.*

HSBC: You seem unsure if the money is going to your wallet or the provider (i.e. the investment fund)? *Mr G: I'm happy to proceed.*

HSBC: We are concerned that this matches a fraud trend...checking is important, suggest you double check, be confident your funds are safe. Are you confident to make the payment? We may not be able to get the money back if it turns out to be fraudulent. *Mr G: yes I am happy to proceed (said twice). Thanks for this due diligence, as always.*

Mr G argues that HSBC didn't go far enough beyond the payments to the crypto wallet – i.e. to ask him more about what happened to the funds being transferred from the crypto wallet onto the fake investment. I've considered carefully what he's said here, but on balance I'm satisfied that HSBC did go far enough. I say that as:

- They gave detailed warnings about scam investments on both calls.
- On the second call, they said they were concerned about the payment and the answers Mr G had given – and re-checked. But Mr G said he wanted to go ahead.
- They asked open questions about the purpose of the payments – and Mr G said he knew what he was doing.
- They asked him about the overall scheme and the role of the loan for £5,000.
- They could see there had been a credit for £5,891 from Mr G's crypto wallet. This created a known payee prior to the other transactions.
- He said he was making money from the investments.
- Overall on the calls, Mr G sounded confident that he knew what he was doing and said he had experience of making the payments before.

Recovery: We expect firms to quickly attempt to recover funds from recipient banks when a scam takes place. I looked at whether HSBC took the necessary steps in contacting the bank that received the funds – in an effort to recover the lost money. And here – I couldn't see evidence that this happened. However, I don't think this would've made a difference – as the funds were sent from Mr G's crypto wallet to the scammer's account, and then very likely removed immediately.

Mr G has lost a lot of money. He's explained why the money was important to him, and the impact his losses have had. I was sorry to learn of his circumstances. He will therefore be disappointed by my decision, but I'm not going to ask HSBC to do anything here.

My final decision

I do not uphold this complaint.

Under the rules of the Financial Ombudsman Service, I'm required to ask Mr G to accept or reject my decision before 31 January 2024.

Martin Lord
Ombudsman