

The complaint

Ms G complains that HSBC UK Bank Plc (HSBC) wouldn't refund money she lost in an investment scam.

What happened

What Ms G says:

In May/June 2022, Ms G opened an account with a third-party payment service provider (A) and then moved money into a crypto investment fund, which turned out to be a scam. She said she had been recommended to make the investment by a friend, who had successfully invested in the past. Ms G made six online payments to her account with A as follows:

Date	Beneficiary	Amount
22 July 2022	Payment service provider (A)	£30
25 July 2022	Credit from A	(£70.55)
15 August 2022	Payment service provider (A)	£8,000
1 September 2022	Payment service provider (A)	£4,000
8 September 2022	Payment service provider (A)	£2,406
9 September 2022	Payment service provider (A)	£3,483.50
14 September 2022	Payment service provider (A)	£2,643
Total loss		£20,491.95

Miss G said she had been coerced and persuaded by the scammer to pay more money to the investment. She had now lost the money as it turned out to be an investment scam.

Miss G said HSBC should've done more to protect her – this was a crypto 'investment' and HSBC, as the experts, should've warned her about the potential for a scam, but didn't. She said HSBC were responsible for the loss of her money – under the guidance and codes for protecting customers from scam payments - and should refund it to her.

What HSBC said:

HSBC said the payments were to an account in the name of Ms G with A and were therefore 'me to me'. And so – HSBC said Ms G should raise the issue with A and didn't refund any money.

Our investigation so far:

Ms G brought her complaint to us. Our investigator didn't uphold it. He said HSBC didn't have to refund any money. Ms G made the payments to her crypto wallet and had full control over the money. They were 'me to me' transactions, and therefore weren't covered under the Contingent Reimbursement Model code (CRM Code).

He said HSBC did stop the first payment of £8,000 – and spoke to Ms G about it. On the call, Ms G was questioned about the payment and HSBC gave her scam warnings, but she still went ahead with the payment. As Ms G had verified the first (and largest) payment, he could see why the subsequent payments were allowed to go through. But – even if HSBC had intervened, based on the call, he was persuaded that Ms G would've gone ahead with the other payments in any case.

Ms G didn't agree and asked that an ombudsman look at her 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 Ms G has lost money in a cruel scam. It's not in question that she authorised and consented to the payments in this case. So although Ms G didn't intend for the money to (eventually) go to a scammer, she 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 Ms G's own account with A.

I need to decide whether HSBC acted fairly and reasonably in its dealings with Ms G when she 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 Ms G normally used her account – then we would expect HSBC to have intervened and spoken to Ms G about them. I looked at Ms G's account, and it's fair to say that the payments were unusual compared to the way in which she used her account – which was to receive her salary and make day to day expenditure of low value. There were three payments for £5,447.18, £1,909.64, and £3,243.31 in December 2021 – but other than those, there weren't any large payments of the value she made in August-September 2022.

We wouldn't have expected HSBC to have intervened in the first, small payment of £30.

But – given the nature of Ms G's account history, HSBC should've intervened in the large payment of £8,000 on 15 August 2022, and they did. HSBC held the payment and spoke to Ms G. I listened the call, and I quote some key parts of it – as it is important in the context of this complaint.

I found the call to be thorough, and HSBC's call handler asked Ms G several open, probing questions about the payment, and gave her sufficient warnings.

HSBC call handler: *We want to protect customers from losing money – why do you want to make this payment?* Ms G replied: *it's to my crypto currency account.*

HSBC call handler: *explain the purpose of this payment/what is the reason for the payment?*
Ms G: *for my crypto currency account, as an investment.*

HSBC call handler: *how long have you had an account with A?* Ms G: *about a month.*

HSBC call handler: *how was the account opened?* Ms G: *via a broker who helped me open it via the app.*

HSBC: *Have you made payments in the past to this beneficiary?* Ms G: *yes.*

HSBC: *Did you pay anything to the broker, a fee?* Ms G: *no.*

HSBC: *Have the previous payments been credited to your account with A?* Ms G: *yes.*

HSBC: *Has anyone told you how to answer our questions, or how to mislead us in any way?*
Ms G: *no.*

HSBC: *We have seen scammers (like this) – are you making an investment into a scheme promising significantly higher returns?* Ms G: *yes.*

HSBC: *What checks have you carried out to verify the legitimacy of this company?* Ms G: *recommended by a friend who's also with them.*

HSBC: *If this is a crypto investment have you made sure you are making payment directly to the provider?* Ms G: *yes.*

HSBC: *Is the online wallet in your name only and only you can access it?* Ms G: *yes.*

HSBC: *Have you seen all HSBC's fraud warnings online?* Ms G: *yes.*

HSBC: *Will you be making any more payments to this beneficiary in the future?* Ms G: *maybe, can't say right now.*

HSBC: read out a scam warning – *criminals are using sophisticated investment scams with the aim of getting unsuspecting people to hand over money, they seem genuine and knowledgeable, always check the beneficiary.....we may not be able to recover any payments made.* Ms G: *I agree.*

HSBC: *Do you want to proceed, or do you want more time to consider and conduct further checks?* Ms G: *I'd like to proceed.*

HSBC: *HSBC will not be liable for any subsequent losses.*

The payment was then released.

I'm satisfied that HSBC asked all the necessary questions, received positive answers from Ms G, and gave warnings - and Ms G confirmed she was happy to go ahead. Therefore, I don't reasonably hold HSBC responsible for Ms G's loss of the payment of £8,000.

I then considered the subsequent payments. These were of a much lower value – and the obligations of HSBC were therefore less. And 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 subsequent payments.

HSBC could also see that the subsequent payments were to the same beneficiary as the earlier large payment of £8,000, so we wouldn't have expected them to question them. And even if HSBC had intervened – such were the responses from Ms G on the first call in August 2022 – that I'm persuaded she would've gone ahead anyway.

So – in the circumstances of this case, I don't hold HSBC liable for the payments made.

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 funds. Ms G contacted HSBC on 12 December 2022. I can see that HSBC then contacted A on 22 December 2022, but no funds remained – as Ms G had moved them into the scam investment well before then. I'm satisfied that HSBC did what we would've expected to try to get the money back.

I'm sorry Ms G has had to contact us in these circumstances. I accept she's been the victim of a cruel scam, but I can't reasonably hold HSBC responsible for her losses. **(continued – final decision below)**

My final decision

I do not uphold this complaint.

Under the rules of the Financial Ombudsman Service, I'm required to ask Ms G to accept or reject my decision before 18 October 2023.

Martin Lord
Ombudsman