DRN-5023502

## The complaint

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

## What happened

*What Mr U says:*

Mr U is represented by a third-party firm of solicitors. He is retired. He saw a pop-up advertisement on his mobile phone which apparently gave an investment opportunity with guaranteed returns. He thought this would be a good way to add to his pension income.

He followed the instructions and registered his interest. He got a call back from someone and was instructed to follow the link to the investment firm (which I call 'firm A').

Mr U followed the person's instructions and downloaded several apps on his phone. He was guided how to send funds – the person got him to download screen sharing software and because he could then see Mr U's screen, told him what keys to press.

Mr U says he was not computer literate and had no investment experience.

He admits he didn't do any research into firm A, and believed what he was told.

Between 10 May 2023 and 2 June 2023, he sent £31,000 in three payments to the scammer firm. Each time, the instructions to Mr U were done on the phone and - the scammer used the screen sharing software to aid Mr U.

Mr U was then told he had made some trading losses and needed to make them up. And then, when he wanted to withdraw funds, he was told he had to pay another £14,000 – he then realised he had been scammed.

Then later, in June 2023, he was contacted by another person – who said she could help him recover the money he lost previously. She said Mr U needed to pay fees to do this – and again, the second scammer was given access to Mr U's phone using screen sharing software. So, he paid a further £200 and £5,000 - the recovery scam.(**continued)**

The payments were:

| Date | Payment | Amount |
|---|---|---|
| 10 May 2023 | Faster payment: crypto exchange account in Mr U's name | £20,000 |

| | | |
|---|---|---|
| 11 May 2023 | Faster payment: crypto exchange account in Mr U's name | £9,000 |
| 2 June 2023 | Faster payment: crypto exchange account in Mr U's name | £2,000 |
| 19 June 2023 | *Recovery scam:* debit card: named personal account | £200 |
| 5 July 2023 | *Recovery scam:* faster payment: crypto exchange account in Mr U's name | £5,000 |
| **Total** | | **£36,200** |

As a result of the scam, Mr U lost most of his life savings – which he was planning to leave to his family when he passes away. He is now struggling to pay bills and has cut back on living expenses. He no longer has the money he wanted to leave to his family. His blood pressure has become worse and for some months, couldn't sleep at night.

Mr U says HSBC should've done more to protect him. The payments were unusual, but the bank didn't intervene or contact him. If HSBC had done so, the scam would've been uncovered. Mr U hadn't been coached to mislead the bank and would've been honest in his answers. Mr U (through his advisors) says he was vulnerable at the time – he was aged 79 and was suffering from high blood pressure and other ailments. He says that had HSBC contacted him the bank would've gain the view he was vulnerable.

Mr U says HSBC should refund the money he's lost plus interest at 8% per annum and compensation of £300.

*What HSBC said:*

HSBC didn't refund any money. The bank said the funds were sent to an account in Mr U's name which he had control over. So – he should contact the crypto exchange for a refund. The bank said Mr U didn't do any research into firm A before going ahead with the payments.

*Our investigation so far:*

Mr U brought his complaint to us. Our investigator upheld it and said:

- Mr U made the payments under instructions from the scammers.
- HSBC should've intervened in the payment for £20,000 – this was much larger than any other payment in the last 12 months; was to a new payee; and he had transferred into the account similar credits on the same day.
- There was minimal evidence of correspondence between Mr U and the scammers, but she was satisfied that Mr U was given the instructions to follow, including downloading several apps on his phone and also screen sharing software.
- He didn't know what he was investing in or what returns he might get.
- So, if HSBC had asked Mr U questions about the payment, it was unlikely that he could've answered any of the bank's questions.
- She considered whether Mr U should be responsible for some of his losses. He didn't carry out any research into firm A or any of the app providers.
- But even if he had, she couldn't see there were any online warnings about them at the time.
- So, she was satisfied that Mr U was manipulated and taken advantage of by the scammers – both in the first scam, and the recovery scam.

- She said HSBC should refund all the money (£36,200) plus interest at 8% per annum.

Mr U accepted this but HSBC didn't. The bank said:

- There was evidence that Mr U was coached. And so even if HSBC had spoken to him, he would've gone ahead anyway.
- In any case, Mr U should be responsible for some of his losses – as he didn't carry out any research; and he acted on an advert on social media, which was known to be unreliable; and he gave the scammers access to his phone, which wasn't a very wise thing to do.

Our investigator disagreed and so HSBC asked that an ombudsman look at Mr U's complaint - so it has come to me.

**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 U 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 U 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.

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

The Lending Standards Board Contingent Reimbursement Model Code (CRM Code) provides for refunds in certain circumstances when a scam takes place. But – it 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 U's own account with the crypto exchange.

If the payments were of a sufficient size and were out of character with how Mr U normally used his account – then we would expect HSBC to have intervened and spoken to him about them. I looked at Mr U's account, and it's fair to say that the payments were unusual compared to the way in which he used his account – it was used to receive his weekly state pension and make small value payments for day-to-day living expenses: usually there were only two/three debit card payments each month and for less than £50. There were two regular standing orders for £250 per month to savings accounts.

Given that, the payment for £20,000 on 10 May 2023 was very unusual – and it was followed by another one for £9,000 the next day. So, Mr U paid £29,000 in two days – which was out of character for him.

Each payment was funded the same day by like credits into Mr U's account. Given that the payments were very unusual, I think it's reasonable to have expected HSBC to hold them and contact Mr U – which the bank didn't.

HSBC was the expert in such matters and if they'd intervened, held the payments and contacted Mr U we would have expected them to ask open questions such as:

- Why are you making the payment?
- Who to?
- For what purpose?
- How did you hear about the investment?
- How were you contacted about it?
- Where did the money come from that you're investing?
- Where is the money going to from your crypto wallet?
- What do you know about crypto investing?
- Have you made crypto investments before?
- How were you given the bank account details where the money was to be paid to?
- Have you given control on your devices to anyone else?

I listened to the calls between HSBC and Mr U which took place after he scam – on 7 August 2023. Because there was so much confusion as to what had happened in the first call, HSBC (sensibly) asked Mr U to go to a branch to explain – and there were then two calls between HSBC' s fraud team, and the branch the following day – with Mr U present. I listened to those calls also.

For me, it is very clear that Mr U was completely deceived by the scammers. He said on several occasions that he 'had no clue' what he was doing, or what he was investing in. He stated that the scammers got him to download several apps and screen sharing software.

They then directed him as to which keys to press on his phone - to send the money from his HSBC savings account to his HSBC current account and then to the crypto exchange. And from there to the scammer firm A. He said he had no idea what the crypto exchange was – he hadn't heard of them. He admitted he didn't carry out any research.

My firm sense of listening to the calls is that had HSBC intervened – as they reasonably should have – then the scam would've quickly unravelled. I don't think Mr U could've given HSBC any answers to even the most the basic of questions we would've expected the bank to ask. And therefore I think it is likely that the bank would have refused to process the payments – and quite possibly asked Mr U to go to a branch to discuss matters. I'm persuaded that it would have become evident very quickly that Mr U was vulnerable and confused. And so I'm satisfied the scam would've been stopped at that time.

HSBC have argued that Mr U was being coached and therefore would not have been truthful in any call. I considered this point – but I'm persuaded that he would not have been able to deceive HSBC in that way. And while I agree he was told which keys to press to make the payments, this isn't 'coaching' in the way we might normally see from scammers - which is when they get customers to mislead the bank as to the true purpose of a payment. This wasn't the case here.

I also considered whether we have seen enough evidence of the scam – and it is fair to say we've seen only a few basic emails. Mr U says most communications were by phone. We approached the crypto exchange and have seen statements which show the transfers in from HSBC and then the purchase of crypto currency - so on balance, I'm satisfied there was a scam and the losses were as stated.

*Contributory Negligence:*

But that's not the end of the story here. I also considered whether Mr U could've done more to protect himself and whether he should therefore reasonably share some of his losses.

In thinking about this - we apply a test of what we would expect a 'reasonable person' to do in the circumstances. We don't (for example) apply a test of what we would expect a finance professional to do.

HSBC argued strongly that Mr U should be partly responsible - because as he didn't carry out any research; he acted on an advert originated social media, which was known to be unreliable; and he gave the scammers access to his phone, which wasn't a very wise thing to do.

So, I considered these points – which are well made by the bank. But in this case, it's clear that Mr U was vulnerable. He was aged 79 at the time (now 80). The phone calls persuade me to conclude he was very confused and exploited by the scammers. And because of his vulnerability, I don't think he was able to carry our online searches of firm A (or the other apps he downloaded). I looked online – and couldn't find any warnings at the time of the scam. So, even if Mr U had looked, I don't think he would've found anything which could have stopped the scam.

And he believed what he was being told on the phone by the scammers. I'm also mindful that Mr U could've been protected by HSBC if the bank had intervened – as it's reasonable they should have.

So, I'm persuaded that it would not be fair or reasonable to ask Mr U to contribute to his losses in the circumstances of this case.

*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, the funds went from the bank account to a crypto currency merchant and the loss occurred when crypto was then forwarded to the scammers. In this case, as the funds had already been forwarded on in the form of cryptocurrency there wasn't likely to be anything to recover.

Therefore based on the evidence I've seen; HSBC should refund £36,200 plus interest of 8% per annum to Mr U.

## My final decision

I uphold this complaint. HSBC UK Bank Plc must:

- Refund £36,200 to Mr U, plus interest at 8% per annum simple from the date of the payments to the date of settlement.

Under the rules of the Financial Ombudsman Service, I'm required to ask Mr U to accept or reject my decision before 20 May 2025.

Martin Lord
**Ombudsman**