

## The complaint

Ms B complains that HSBC UK Bank Plc won't refund money she lost when she fell victim to an investment scam.

Ms B is being represented by solicitors in this complaint.

## What happened

The detailed background to this complaint is well known to the parties and has been previously set out by the investigator. The facts about what happened aren't in dispute. So, I'll focus on giving my reasons for my decision.

The complaint concerns three transactions totalling £12,200 which Ms B made using her HSBC debit card in August 2023. She states these were made in connection with an investment opportunity provided by company, "X", whose advertisement she came across on the internet several weeks prior.

Ms B initially (July 2023) made deposits via her account with "R", an electronic money institution. She transferred funds from her HSBC account to R, before purchasing cryptocurrency from a cryptocurrency exchange. It was then sent on to cryptocurrency wallets as instructed by her 'account manager'. At the time Ms B thought she was loading it on to her account with the investment platform as the balance went up accordingly.

When she experienced some difficulties with making deposits via R, under her account manager's advice, Ms B reverted to making deposits from her HSBC account. She purchased cryptocurrency from a cryptocurrency provider "M", before sending it on to wallets as instructed by her account manager.

The following transactions are relevant to this complaint:

	Date	Type	Payee/details	Amount
Payment 1	1 August	Debit card	Ms B's wallet with M	£150.00
	1 August	Credit	M	£134.45
Payment 2	16 August	Debit card	Ms B's wallet with M	£8,522.00
Payment 3	17 August	Debit card	Ms B's wallet with M	£3,528.00
			<b>Total loss</b>	<b>£12,065.55</b>

In September 2023, when her investment account required further deposit to avoid losing everything, Ms B states she researched X further. It was then that she noticed negative reviews and a recent warning published by the Financial Conduct Authority.

This decision solely relates to Ms B's complaint about HSBC. Her concerns about R's acts and omissions, from where she initially made the scam payments, have been considered separately by our service.

Our investigator didn't uphold the complaint as they didn't think HSBC should reasonably have been expected to prevent the payments. They explained that the payments weren't particularly unusual or suspicious considering previous account activity, and there was no interaction between Ms B and HSBC at the time such that an opportunity was missed. The investigator also said that the payments went to M, not X, and there were no warnings about M.

Ms B's representative has asked for the matter to be decided by an ombudsman. In summary, it disagrees that the larger transactions in dispute are in line with normal account spending. The representative also states that an opportunity was missed when HSBC failed to contact Ms B to speak about the disputed transactions.

I issued my provisional decision last month and gave reasons for why I didn't intend upholding this complaint. I gave both parties an opportunity to provide further comments and arguments before finalising my decision.

HSBC replied and said it didn't have anything further for me to consider. We haven't heard back from Ms B's representative despite sending a reminder. As the deadline I gave has since passed, it's appropriate for me to proceed to issue my final decision.

What follows is my provisional decision made final.

### **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'd like to start by saying I'm sorry to hear about Ms B's personal circumstances and how this incident has impacted her. I'd like to reassure Ms B and HSBC that although I've only summarised the background above, so not everything that's happened or has been argued is detailed, I have read and considered their submissions in their entirety.

It's not in question that Ms B was the victim of a cruel scam and it's very unfortunate that she's lost money. But HSBC doesn't automatically become liable to reimburse her loss.

Under regulations and in accordance with general banking terms and conditions, banks should execute an authorised payment instruction without undue delay. The starting position is that liability for an authorised payment rests with the payer, even where they are duped into making that payment. There's no dispute that Ms B made the payments, and so they are authorised.

But in accordance with the law, regulations and good industry practice, a bank should be on the look-out for and protect its customers against the risk of fraud and scams so far as is reasonably possible. If it fails to act on information which ought reasonably to alert a prudent banker to potential fraud or financial crime, it might be liable for losses incurred by its customer as a result.

I don't consider the first payment ought to have appeared as unusual or suspicious to HSBC. It was low in value, and I don't think HSBC should reasonably have suspected that it might be part of a scam.

However, Payment 2 was relatively larger. While agree with the investigator that Ms B's account history shows multiple payments for similar or larger values in the 12 months prior to the scam payments, I think HSBC should have identified that the payment was identifiably cryptocurrency related (the merchant is a well-known cryptocurrency provider). I accept that

buying cryptocurrency is a legitimate exercise. But by August 2023, when Ms B's payments were made, there had been an increased prevalence of investment scams involving cryptocurrency. Both the financial services regulator and Action Fraud had warned of cryptocurrency scams. This type of insight is something that regulated businesses, including HSBC, ought to take notice of.

Given the sudden jump in cryptocurrency related spending, I consider HSBC should have identified that Ms B was at heightened risk of financial harm from fraud. In line with good industry practice and regulatory requirements, I'm satisfied that it is fair and reasonable to conclude that the bank should have warned its customer before this payment went ahead. HSBC has told us that no such warnings were provided.

I've thought carefully about what a proportionate warning in light of the risk presented would be in these circumstances. In doing so, I've taken into account that many payments that look very similar to this one will be entirely genuine. I've given due consideration to HSBC's primary duty to make payments promptly.

I think that by August 2023, when these payments took place, HSBC should have had systems in place to identify, as far as possible, the actual scam that might be taking place and to provide tailored, effective warnings relevant to that scam. I accept that any such system relies on the accuracy of any information provided by the customer and cannot reasonably cover off every circumstance. But I consider that by August 2023, on identifying a heightened scam risk, a firm such as HSBC should have taken reasonable steps to attempt to identify the specific scam risk – for example by seeking further information about the nature of the payment to enable it to provide more tailored warnings.

In this case, HSBC knew that the Payment 2 was being made to a cryptocurrency provider and its systems ought to have factored that information into the warning it gave. The bank should also have been mindful that cryptocurrency scams have become increasingly varied over the past few years. Fraudsters have increasingly turned to cryptocurrency as their preferred way of receiving victim's money across a range of different scam types, including 'romance', impersonation and investment scams.

Taking that into account, I'm satisfied that, by August 2023, HSBC ought to have attempted to narrow down the potential risk further. I'm satisfied that when Ms B made the payment in question, HSBC should – for example by asking a series of automated questions designed to narrow down the type of cryptocurrency related scam risk associated with the payment she was making – have provided a scam warning tailored to the likely cryptocurrency related scam Ms B was at risk from.

In this case, Ms B was falling victim to an investment scam. As such, I'd have expected HSBC to have asked a series of simple questions in order to establish that this was the risk the payment presented. Once that risk had been established, it should have provided a warning which was tailored to that risk and the answers Ms B gave. I'd expect any such warning to have covered off key features of common cryptocurrency investment scams, for example referring to: an advertisement on social media, promoted by a celebrity or public figure; an 'account manager', 'broker' or 'trader' acting on their behalf; the use of remote access software and a small initial deposit which quickly increases in value.

But had HSBC done so, I'm not persuaded that the warning would have prevented Ms B's loss. I'll explain why.

Just weeks prior to the suggested intervention point, a payment Ms B had attempted to send (also to purchase cryptocurrency) from her e-money account with R was declined. After informing her that this was due to the payment being highly likely scam related, based on

another customer confirming a very similar transaction as a scam, R went on to make further enquiries. Ms B reached out to the scammer, who she was in regular contact with, and asked for help in answering R's questions. She confirmed she was buying cryptocurrency but, amongst other things, also said she was experienced in trading and had over four years' experience. Ms B confirmed that she hadn't seen anything advertised and was carrying out the transaction by herself without involvement from anyone else.

We know some of the responses provided weren't true. For instance, she had come across the X through an advertisement on the internet. And someone was assisting her in purchasing cryptocurrency and the ultimate 'investment'. Ms B didn't have any concerns when she was instructed to mislead R. I'm also mindful that at the time of Payment 2, Ms B had already been investing with X for some time. She's told us she could see her increasing profits during that period. And she hadn't been pressured into putting more funds in by that point – this happened later on.

So, weighing up everything, on the balance of probabilities, I'm not persuaded that a warning by HSBC specific to cryptocurrency investment scams would have positively impacted Ms B's decision making. Contemporaneous evidence shows she turned to the scammer when R made enquiries. I think it's more likely than not that Ms B would have done the same had HSBC intervened at the suggested point, or at the time of the next transaction.

What this means is that I'm not persuaded HSBC could have prevented the transactions Ms B made in relation to the scam.

I've also thought about whether HSBC could have done more to recover the funds once it became aware of the situation, as in some circumstances the money can be recovered. Here, the recovery avenue would have been limited to chargeback. But Ms B's payments went to a cryptocurrency exchange. She wouldn't be able to make a successful chargeback claim in the circumstances because the merchant she paid did provide the service requested (i.e., conversion of fiat money into cryptocurrency).

To summarise, I'm not persuaded that any failure on HSBC's part is the proximate cause for Ms B's loss. I fully acknowledge that she's lost a lot of money, and this has had a huge impact on her. But having considered the matter very carefully, for the reasons given, it wouldn't be fair of me to hold HSBC responsible for her loss.

### **My final decision**

For the reasons given, my final decision is that I don't uphold this complaint.

Under the rules of the Financial Ombudsman Service, I'm required to ask Ms B to accept or reject my decision before 13 December 2024.

Gagandeep Singh  
**Ombudsman**