DRN-5248748

The complaint

Mrs N complains that HSBC UK Bank Plc (HSBC) won't refund her after she was the victim of a scam.

What happened

Mrs N was contacted via a popular messaging platform and was told about a part-time job she could perform from home. Mrs N had been looking for a part-time job and had contacted a number of recruitment agencies, so this contact didn't seem particularly unusual. She researched the company, which seemed to have good reviews and appeared to be legitimate and she was told how the job worked. This involved completing various tasks that made various apps appear more popular, which would earn Mrs N commission. She was told she would have an account with the company, where her commission would be paid and she might need to top-up the account, as the account would need a positive balance before she would be able to withdraw her earnings.

Mrs N made the following payments to her own cryptocurrency account:

Date	Payment type	Amount
2 June 2023	Faster payment	£26.84
5 June 2023	Debit card payment	£40.00
5 June 2023	Debit card payment	£10.00
8 June 2023	Debit card payment	£1,000.00
8 June 2023	Debit card payment	£2,150.00

But Mrs N was unable to make withdrawals and was asked to make more payments to her account and she says she then realised this was a scam.

Mrs N says HSBC ought to have intervened because there were a number of factors that were suspicious. In particular, she says this was a series of unusual transactions; of increasing value; to a new payee; which was a cryptocurrency provider; and the payments were made in rapid succession. She also suggests she spoke to HSBC, before the £2,150 payment was made and told it that she needed to make the payment to buy cryptocurrency for her job and this ought to have raised suspicions.

HSBC said it flagged the £2,150 payment and texted Mrs N to check she had authorised it and she responded, via text, to confirm she had authorised it. Later that day, she called HSBC to report the scam, as the scammers had asked for further amounts. HSBC refunded the £26.84 transaction, as a gesture of goodwill.

Our investigator didn't uphold Mrs N's complaint. He considered that the transactions weren't suspicious and didn't think they ought reasonably to have caused HSBC to intervene. He was satisfied HSBC didn't have a basis on which it could attempt to recover the money, as most of the payments had been made by debit card and had funded Mrs N's own account with a legitimate cryptocurrency provider. As such, he didn't consider there was any prospect of HSBC making successful chargeback claims.

I issued a provisional decision on 18 November 2024 and said:

"There is no dispute that Mrs N authorised the payments. I appreciate she didn't intend her money to go to scammers. Under the Payment Services Regulations 2017, she is liable for the loss in the first instance. But the matter doesn't end there.

In this case, the Contingent Reimbursement Model code does not apply because the transactions were between two accounts held by Mrs N and it also doesn't apply to debit card payments. However, taking into account the law, regulatory 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 made 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.*

Having considered all the available evidence, I agree with the investigator that the pattern of transactions wasn't particularly unusual, to the extent it ought to have prompted HSBC to intervene further than it did. There were five transactions over the course of six days, rather than a series of rapid transactions, her HSBC account was well-funded and the payments didn't drain the account. Mrs N had made several higher-value payments in the months before, so payments of £1,000 and £2,150 wouldn't have appeared particularly out of character. While Mrs N says her other high-value payments were to her own business, high-value payments appear to have been made to several payees and not all to Mrs N's business.

The payments were to a cryptocurrency provider and I would expect firms to be aware there's an elevated risk with these transactions, and the payments on 8 June 2023 total a fairly high amount. But even if I were to find that HSBC should've intervened more than it did, due to the payment destination and cumulative value, I consider a proportionate intervention would likely have been a tailored, written warning of some of the key features of cryptocurrency investment scams. Such a warning is unlikely to have caused Mrs N concern or halted the scam she was falling victim to because she didn't think she was investing – she thought she was working.

Overall, I'm not persuaded the transactions were unusual enough that HSBC ought to have been prompted to intervene further and I don't consider the intervention HSBC did make, by text message, was inappropriate. But for the reasons given, even if a further, reasonable intervention had been made, I consider it unlikely it would have prevented Mrs N's loss.

Mrs N suggests there was a telephone conversation before the £2,150 payment was released. She says HSBC asked her what the payment was for; she told it she had started a new job; and she'd been asked to transfer money in order to access her earnings. She said she spoke to HSBC and its staff could hear she was confused.

The only available call appears to be the one that took place on 8 June 2023, after the final transaction was authorised. HSBC says the last payment was released following Mrs N's text message confirmation that she had authorised the payment. During the call with HSBC on 8 June 2023, when Mrs N reported the scam, there is no reference to an earlier conversation. HSBC advised it couldn't stop this payment, even though it had been made a short time earlier. The payment shows on Mrs N's account statement as having debited her account on 9 June 2023, which was after the call and may be the source of any confusion, but the payment was authorised on 8 June 2023. On balance, I've seen insufficient evidence of a call before the payment was authorised.

I should also note that despite the investigator asking for evidence of contact between Mrs N and the scammers, no evidence of contact between Mrs N and the scammers has been provided, so there is very little evidence to show Mrs N has been the victim of a scam or that she has suffered a financial loss and is unable to access the money she paid. On that basis, even if I had been persuaded that HSBC ought to have intervened more than it did, I don't consider I could reasonably uphold a complaint against HSBC that it is responsible for any loss Mrs N might have suffered when insufficient evidence has been provided to show a fraud has taken place and a loss has occurred.

Mrs N responded to my provisional decision. She said she is suspicious why HSBC has not provided a copy of the recording of the telephone call on 8 June 2023, before the last payment was made. HSBC could hear she was confused, she told HSBC it might be a scam but the scammers promised to pay her and she believed them.

HSBC should have spotted high payments and prevented her from paying the last two transactions. Previous payments had only been made to her business account and these payments reduced the balance of her account quite significantly.

Mrs N also provided some evidence of her interactions with the scammers.

HSBC didn't comment on my provisional 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.

Mrs N has now provided some evidence showing her interactions with the scammers and indicating that she has suffered loss as a result of the scam.

But having considered everything, and Mrs N's further comments and submissions, I remain of the view that the pattern of transactions wasn't sufficiently unusual that I would have expected HSBC to have intervened. While the transactions do appear to have been made to a cryptocurrency provider, it's not clear that this would have been apparent to HSBC at the time and the transactions were not particularly large or frequent. As mentioned, other similar sized payments had been made from the account before.

Even if I were to conclude that HSBC ought to have intervened in the transactions, I consider a proportionate intervention at that time would have been to give a tailored written warning about investment scams, if HSBC was able to identify the payments were being made to a cryptocurrency provider. I consider it unlikely such a warning would have caused Mrs N to act differently because she didn't think she was making an investment, rather that she was making a payment in connection with her work.

While there appears to be some confusion about the sequence of events surrounding the call with HSBC, I'm satisfied the phone call to HSBC was made after Mrs N had authorised the final transaction and there was no way for HSBC to stop the payment by the time Mrs N spoke to it.

For those reasons, I don't think HSBC is responsible for Mrs N's loss and so I don't require it to do anything more.

My final decision

I don't uphold Mrs N's complaint.

Under the rules of the Financial Ombudsman Service, I'm required to ask Mrs N to accept or reject my decision before 5 February 2025.

Greg Barham
Ombudsman