DRN-5150318

The complaint

Miss N complains that HSBC UK Bank Plc ('HSBC') won't refund the money she lost as the result of a scam.

What happened

In 2022, Miss N was made aware of an investment opportunity with a company I'll refer to as V.
Miss N had to purchase cryptocurrency, which she sent to V as part of the investment.

These are the payments Miss N made from her HSBC account to purchase cryptocurrency. Both B and P offer cryptocurrency exchange services.

Date	Details of transaction	Amount
24.11.2022	Card payment to B	£1,000
28.12.2022	Card payment to B	£850
3.7.2023	Open banking payment to P	£10
4.7.2023	Open banking payment to P	£190
20.7.2023	Open banking payment to P	£200
11.8.2023	Open banking payment to P	£250
11.8.2023	Open banking payment to P	£400
12.8.2023	Open banking payment to P	£500
13.8.2023	Open banking payment to P	£500
14.8.2023	Open banking payment to P	£500
15.8.223	Open banking payment to P	£500
22.8.2023	Open banking payment to P	£500
30.8.2023	Open banking payment to P	£500
5.10.2023	Open banking payment to P	£1,000
12.10.2023	Open banking payment to P	£1,000
19.10.2023	Open banking payment to P	£1,000
22.10.2023	Open banking payment to P	£1,000
25.10.2023	Open banking payment to P	£1,000

Miss N raised a fraud claim with HSBC in May 2024, through a professional representative. Miss N says the investment was a scam.

HSBC considered Miss N's claim but declined to refund her. HSBC said the funds were sent to cryptocurrency wallets held in Miss N's name and they aren't liable for her loss. With regards to the two card payments, the dispute was raised outside of the time limits set for chargeback and wouldn't have been successful as Miss N got what she paid for – cryptocurrency.

Miss N wasn't happy with HSBC's response, so she brought a complaint to our service.

An investigator looked into Miss N's complaint but didn't uphold it. The investigator explained that Miss N's payments aren't covered by the Contingent Reimbursement Model Code (CRM

Code) as the funds went to accounts in her own name. Based on the size and frequency of the payments, the investigator didn't feel HSBC should've identified a risk of financial harm or intervened when the payments were made.

Miss N disagreed with the investigator's view and asked for an ombudsman to review her case. She raised the following points:

- Had HSBC intervened and asked questions, they would've identified that she wasn't an experienced investor, and the scam would've been uncovered. So, HSBC missed the opportunity to prevent her loss.
- If HSBC had provided a warning when the payments were made, Miss N wouldn't have proceeded with making the payments.

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.

In deciding what's fair and reasonable in all the circumstances of a complaint, I'm required to take into account relevant: law and regulations; regulators' rules, guidance and standards; codes of practice; and, where appropriate, what I consider to be good industry practice at the time.

Where there is a dispute about what happened, and the evidence is incomplete or contradictory, I've reached my decision on the balance of probabilities. In other words, on what I consider is more likely than not to have happened in light of the available evidence.

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 (in this case the 2017 regulations) and the terms and conditions of the customer's account.

Here it's not in dispute that the payments were authorised, albeit Miss N did so not realising she was the victim of a scam – but that doesn't make the payments unauthorised. So, the starting position is that HSBC isn't liable for the transactions.

There are however, some situations where we believe that businesses, taking into account relevant rules, codes and best practice standards, shouldn't have taken their customer's authorisation instruction at "face value" – or should have looked at the wider circumstances surrounding the transaction before making the payment.

Miss N's card payments and open banking payments aren't covered by the CRM Code, as it doesn't cover payments made between a customer's own accounts. Miss N was purchasing cryptocurrency which was paid into wallets in her own name before it was sent to the scammer, so I can't apply the provisions of the CRM Code.

Should HSBC have intervened when Miss N made the payments?

I'm not satisfied that I can fairly say HSBC should've identified a risk of financial harm from fraud when Miss N made these payments. I say this because:

- While some of the payments were made on consecutive days, they weren't of a high enough value that I think HSBC should've been concerned.

- A lot of the payments were spread out, with days or weeks between payments.
- After the first card payment to B and open banking payment to P, the payments were made to what became an existing payee.
- There wasn't a series of payments made to different payees, or a lot of payments made within the space of a few minutes, which is often seen in the case of fraud.
- The payments weren't so unusual or out of character compared to the previous account activity, that HSBC should've been concerned. Miss N regularly made payments or transfers of up to £500 from her account each month. While the payments for £1,000 were higher than Miss N's usual activity, I'm not satisfied that the payments were so large that I would've expected HSBC to have identified an APP scam risk.

I appreciate that this was a lot of money for Miss N. But HSBC has to strike a balance between identifying payments that could be fraudulent and then responding appropriately based on their concerns, while ensuring minimal disruption to legitimate payments. And, in this case, I'm satisfied that HSBC acted reasonably by following Miss N's payment instructions without intervening.

Miss N says if HSBC had intervened and asked questions the scam would've been uncovered. However, I first have to be satisfied that HSBC should've intervened, before I can consider whether they asked appropriate questions to potentially uncover the scam. In this case, I'm not satisfied that HSBC should've identified a scam risk and intervened, so they weren't required to ask questions.

Chargeback

I wouldn't have expected HSBC to have raised a chargeback as it was unlikely to be successful. I say this because Miss N made the card payments to purchase cryptocurrency, which she received. So, she got what she paid for. Chargeback doesn't look at the end destination of the funds, it only looks at the initial transaction, which in this case is the purchase of cryptocurrency. On that basis, I'm satisfied that HSBC acted reasonably in not raising a chargeback.

Recovery of funds

As the funds were used to purchase cryptocurrency, which was paid into wallets in Miss N's name, HSBC couldn't have recovered the funds. If any funds remained in Miss N's cryptocurrency wallets, she would've had access to them.

Compensation

Miss N has asked for £1,000 compensation but hasn't said why she isn't happy with the service she's received from HSBC. As I'm not satisfied that HSBC has provided a poor level of service, I can't fairly make a compensation award.

I'm really sorry to disappoint Miss N, but I'm not satisfied that I can fairly hold HSBC liable for her loss or ask them to refund her.

My final decision

My final decision is that I don't uphold this complaint against HSBC UK Bank Plc.

Under the rules of the Financial Ombudsman Service, I'm required to ask Miss N to accept or reject my decision before 14 July 2025.

Lisa Lowe
Ombudsman