DRN-5807236

The complaint

Mrs J and Mr J complain that HSBC UK Bank Plc won't refund the money they lost to an investment scam. Mrs J and Mr J are represented in this complaint, but I'll refer to them as it's their complaint.

What happened

There is limited information on the events that occurred. Mrs J and Mr J explain that:

They were either contacted on their messaging app by a broker (the scammer) or found them on the messaging app upon viewing a celebrity endorsement. The broker claimed they could earn large returns on crypto investments. They persuaded Mrs J and Mr J to invest into crypto and showed them fake real time returns, stock tickers tracking real market movements and the deposits loaded onto a platform. This encouraged further investment.

They made the following three payments to Company P, paying them from legitimate crypto exchange Company B which they credited from their HSBC account.

Transaction Number	Date	Payment Method	Payee	Amount
1	21/06/21	Faster payment	Mr J's account with Company B (crypto exchange)	£2,000.00
2	22/06/21	Faster payment	Mr J's account with Company B (crypto exchange)	£10,000.00
3	24/06/21	Faster payment	Mr J's account with Company B (crypto exchange)	£2,000.00
Total				£14,000.00

The scammer guided them to open a Company B account and Mrs J and / or Mr J gave them access to their computer.

When they tried to withdraw funds, the scammer(s) asked for further fees in order to do so, and this is when they realised it was a scam.

Mrs J and Mr J complained to HSBC in May 2025. They said HSBC should've intervened on payment 2 for £10,000 as it was out of character and, if they had, they would've been able to identify many hallmarks of a standard cryptocurrency trading scam. This included:

- *'The payments were being sent to an unregulated third party through a cryptocurrency exchange, which matches exactly what Action Fraud warned about in 2018.*
- *The broker was giving financial advice, for which they aren't regulated.*
- *It was unrealistic that they felt that they could make high returns.'*

Also, they said they were inexperienced investors including in crypto and were vulnerable at the time having due to having become parents.

HSBC rejected the complaint and refund claim saying the payments Mr J made weren't eligible for a refund under the Contingent Reimbursement Model (CRM) as the funds were sent to their own account.

Mrs J and Mr J brought their complaint to our service, but our investigator couldn't see evidence of a scam and wasn't persuaded that HSBC had done anything wrong.

As Mrs J and Mr J remain dissatisfied their complaint has been passed to me to look at.

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, I am required to take into account relevant law and regulations, regulators' rules, guidance and standards, and codes of practice; and, where appropriate, I must also take into account what I consider to have been good industry practice at the time.

Having done so, whilst I don't disbelieve Mrs J and Mr J's account of what happened and I'm very sorry to hear they've lost a significant amount of money here, my key findings in this case are that there is:

- A lack of evidence that money was paid to Company P (via company B) and a scam occurred. This is despite our investigator providing sufficient time and opportunity for evidence to be presented.
- Evidence that HSBC recognised a risk, put in place an effective intervention, providing relevant warnings which were both read and accepted and could've prevented payments being made to Company P (via company B).

So, I'm not upholding this complaint and asking HSBC to make a refund payment.

Regarding my comments about the evidence in this case, I did take into account Mrs J and Mr J's account of what happened. Whilst I'm sympathetic, don't disbelieve their testimony, recognise the time gap and how this and life events impacted on retention of communications with the scammers and scam Company C, there importantly isn't any evidence of any instructions, what happened to their money after they paid a legitimate crypto company and if and when the funds left Company B. Also, there isn't any evidence that HSBC were aware of their vulnerability and any request they made to discuss the risks and mitigation.

So, even if I were satisfied that there were failings by HSBC, without this it wouldn't be fair or reasonable to require them to make a refund.

Also, the Lending Standards Board's Contingent Reimbursement Model (CRM) Code, which came out in 2019 and requires firms to reimburse customers who have been the victim of a scam in most circumstances, doesn't apply. This is because:

- The CRM Code sets out the following:
    - Under 'DS1(2) (a)' the scope of what the CRM Code covers in relation to authorised push payment ("APP") fraud in instances where: "(i)The Customer intended to transfer funds to another person, but was instead deceived into transferring the funds to a different person; or (ii) The Customer transferred funds to another person for what they believed were legitimate purposes but which were in fact fraudulent."
    - The payments Mrs J and Mr J made from their HSBC account went to an

account in one of their names. So, it isn't covered by or within the scope of the CRM Code. This is because they weren't paying 'another person'.

Although it isn't relevant, because of the lack of evidence, I did consider the:

Payment Services Regulations 2017 (PSR)

Under the PSR 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 Mrs J and / or Mr J made the payments to Company B, so they are considered authorised. However, 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.

Banks do have to strike a balance between the extent to which they intervene in payments to try and prevent fraud and/or financial harm, against the risk of unnecessarily inconveniencing or delaying legitimate transactions.

So, I consider HSBC should fairly and reasonably:

- Have been monitoring accounts and any payments made or received to counter various risks such as anti-money laundering and preventing fraud and scams.
- Have 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.

It isn't the case here that HSBC didn't intervene or intervened ineffectively. I found that HSBC issued warnings on payment 2 having already sent a check payees warning on the earlier payment. They highlighted with an exclamation mark in a bold amber circle headed '*take care when sending money'* which included the following advice:

A. If an investment sounds too good to be true it could be a scam.

B. Fraudsters can pressurise you to invest.

C. Take time to talk to someone you trust.

D. Check the company is genuine and authorised by the Financial Conduct Authority (FCA) before making any payment.

Points A, B and D all applied to this scam. Point D because the FCA had issued a warning about Company P in August 2020.

Also, HSBC's system required a click and continue action and said 'by doing so you agree you have read our advice'. In addition, there was a fraud centre link. Although I don't have information on the content in 2021, I think it likely this would've included information on investment scams, necessary checks and that HSBC wouldn't ask customers to share information.

I recognise this wasn't a human intervention, but I think this was a strong and relevant warning. Also, it wasn't out of character for Mrs J and Mr J to make a payment for up to

£10,000. In addition, as pointed out by our investigator, in 2021 crypto fraud was in its infancy and there wasn't the post 2023 elevated risk.

So, having considered all the above, I'm sorry to give Mrs J and Mr J disappointing news but I'm also not persuaded that HSBC acted unfairly or unreasonably here and I'm not upholding this complaint.

My final decision

For the reasons set out above, my final decision is not to uphold this complaint against HSBC UK Bank Plc.

Under the rules of the Financial Ombudsman Service, I'm required to ask Mrs J and Mr J to accept or reject my decision before 18 December 2025.

Paul Douglas
Ombudsman