DRN-4694575

The complaint

Ms M complains that Bank of Scotland plc trading as Halifax won't refund money she lost when she fell victim to an employment scam.

Ms M is being represented by solicitors in this complaint.

What happened

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

The complaint concerns several transactions totalling just over £46,000 which Ms M made in July 2023 in connection with a job opportunity – completing tasks – with a company "X" who reached out to her through an instant messaging service. It was explained to her that her job would involve completing the assigned tasks to earn commission.

Ms M's 'trainer' also told her that she would sometimes be granted 'combination tasks', which required a group of tasks to be completed before any withdrawal could take place. Each combination task had a value, given in USDT. Each time a combination task was assigned, the value of the task in USDT would be deducted from Ms M's account balance with X, leaving her with a negative balance. She was told the balance needed to be made positive by depositing USDT in her account before any withdrawals could be made.

In order to make deposits into her account with X, Ms M was instructed to convert her money into USDT. She bought cryptocurrency from a cryptocurrency exchange by making payments from her Halifax account. It was then sent to wallet addresses provided by her trainer. Ms M believed she was making deposits into her account with X, given its account balance went up by the same amount. But before she could make withdrawals, she was given another combination task of a greater value, meaning she would have to complete those tasks (and therefore make another deposit).

This pattern continued for a while and Ms M made further payments despite telling her trainer that she believed the scheme was a scam. She stopped when she didn't have any money left but made a final payment months later in September 2023 as she was desperate to recover her funds. During this time, Ms M was able to make two withdrawals totalling just over £6,000 from the cryptocurrency platform she'd been using.

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.

Having done so, I agree with the conclusions reached by the investigator for the following reasons:

- 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 M made the payments, 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 it to potential fraud or financial crime, the bank might be liable for losses incurred by its customer as a result.

- I've looked at the operation of Ms M's account and, like the investigator, I don't consider the first nine disputed payments, with amounts ranging between £3 and £975, to be *that* unusual. Also, Ms M's account activity shows previous payments to cryptocurrency platforms. Considering these factors, I don't think Halifax ought to have identified that there was a heightened risk of fraud. But by the time Ms M authorised Payment 10 (£3,524), I consider a pattern of increased spending on cryptocurrency activity was beginning to emerge. I think a proportionate response to the risk presented would have been for Halifax, knowing (or strongly suspecting) that the payment was going to a cryptocurrency provider, to have provided a written warning that was specifically about the risk associated with the most prevalent type of cryptocurrency scams, i.e., investment scams.

- But I'm not persuaded that such a warning it would have prevented Ms M's loss. This is because she wasn't sending payments in connection with an investment. She understood she was using the cryptocurrency platform to deposit funds into her account to spend with her 'employer'. So, I'm not satisfied that the kind of warning I would have expected at that time – setting out the typical hallmarks of cryptocurrency investment scams – would have resonated with Ms M.

- Ms M continued sending scam-related payments that day. When she made Payment 13 (£4,000) which was of a similar value, arguably Halifax should have intervened again considering the amount of money Ms M had sent that day in cryptocurrency related transactions. Certainly, by Payment 15 (£8,000), I think the bank should have contacted Ms M and made further enquiries to establish the risk the payment presented before executing her authorised instructions. But, had it done so, I'm not persuaded that such enquiries would have prevented Ms M's loss.

- As the investigator noted, and I agree, the chat correspondence with the scammer shows that Ms M had her own misgivings about employment scheme at the time of the suggested trigger point. Despite telling the scammer that she believed she was being scammed, Ms M went ahead with the payments. On at least two occasions, she discussed her concerns with the scammer on the phone. It's possible that they were able to provide reassurances to Ms M at those times. But it's equally possible, and more likely, that Ms M was desperate to recover her funds. I say this because prior to making Payment 15, she told the scammer that she had discussed the situation with her son, and he believed that she was being scammed. Yet, Ms M carried on making that payment and further payments until she had no funds left.

- Given her state of mind and the sums already lost, on balance I'm not persuaded that a warning from Halifax about job scams involving cryptocurrency would have stopped her in her tracks. It seems that even after engaging the services of a solicitor's firm to help recover her funds, Ms M made a further payment in connection to the scam.

- Thinking next about recovery, given the cryptocurrency Ms M purchased had already been sent on to the scammer, it's unlikely there would have been any funds left to recover. So, I don't think Halifax could or should have done anything further in this regard.

In summary, I recognise that Ms M will be disappointed with this outcome. I understand that the scam has had a significant impact on her wellbeing. I'm sorry that she fell victim to such a cruel scam. But I'm not persuaded that any failure on Halifax's part in not intervening at the suggested trigger points is the proximate cause for Ms M's loss. I fully acknowledge that she's lost a lot of money. But having considered the matter very carefully, for the reasons given, it wouldn't be fair of me to hold Halifax 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 M to accept or reject my decision before 18 February 2025.

Gagandeep Singh
Ombudsman