

## **The complaint**

Miss P complains that Bank of Scotland plc (trading as “Halifax”) won’t refund over £14,000 she says she lost to an employment scam that her partner had fallen victim to.

## **What happened**

The details of this complaint are well known to both parties, so I won’t repeat everything again here. In brief summary, Miss P’s partner (“A”) had been contacted by a scam recruiter (“G”) offering a remote employment opportunity, which involved him having to complete certain tasks online. However, in order to unlock certain tasks, he had to make payment via cryptocurrency, but was assured he would receive more money back as payment for completing the tasks.

Miss P said that A eventually ran out of money, so she offered to help him pay for more tasks so he could receive payment. She opened a cryptocurrency account with Crypto.com where she made several payments to from her Halifax account totalling £16,507.56 between 10 – 11 January 2023. Miss P initially said that she’d transferred her cryptocurrency to the scammer directly in order to unlock further tasks, but later clarified that she transferred her cryptocurrency to A’s Binance wallet, which he then sent on to the scammer in order to unlock the tasks.

Miss P and A realised they’d been scammed when G asked for a further payment to withdraw the money after completing his set number of tasks. She reported the fraud to Halifax and asked it to consider reimbursing the money she’d lost.

Halifax said it wouldn’t refund the money Miss P lost as she’d authorised the payments. It did initially reimburse the first payment of £2,874.82 in error, which it said Miss P could retain as a gesture of goodwill. Unhappy with this, Miss P referred the matter to our service.

Our investigator didn’t uphold the complaint. She didn’t think Halifax could reasonably be held liable for the money lost to the scam, as it was A, rather than Miss P, who had lost his money to the scammers. She also didn’t think an intervention would have likely prevented the loss, even if it could be held liable. Miss P disagreed, so the matter has been escalated to me to determine.

## **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:

- Miss P initially said that she’d transferred her crypto directly to the scammer in order to unlock further tasks for A. But Miss P has since clarified that she transferred her cryptocurrency to A’s Binance wallet (that she did not have access to), which he then sent on to the scammer himself in order to unlock the tasks. It therefore isn’t Miss P that

has suffered a loss to the scam in these circumstances; it was A who lost the money/cryptocurrency that Miss P had either lent or given to him. As such, I'm not persuaded it would be fair and reasonable for Halifax to be held liable for this loss, as Miss P didn't lose her money to a scam; she simply sent it to her partner. I therefore don't consider it necessary to consider whether Halifax ought to have intervened in these circumstances.

- Even if the loss could be considered as Miss P's and I were to agree that Halifax should have made further enquiries, I still don't think it would be fair and reasonable to hold the bank liable in any event. This is because I don't think Halifax could've reasonably foreseen that the money Miss P was sending to a legitimate cryptocurrency exchange platform would then be transferred on again to her partner's crypto wallet only to subsequently be transferred on again to a scammer. As a result, I'm not persuaded legal causation can reasonably be established here.
- Even if the loss could be said to have been foreseeable, the fact that the loss didn't even occur from Miss P's Halifax account or her own crypto wallet – but from another unconnected crypto wallet belonging to her partner – would in my opinion constitute an intervening act that would also serve to break the chain of causation in any event. As a result, I don't consider there to be any fair or reasonable basis in which Halifax could be held liable for the money Miss P paid to her own crypto account that she then sent to her partner.
- I also note that Miss P was not forthcoming with the true nature of the payments when she reported the scam to Halifax either. Despite being under the impression that A was employed by G, and that she was sending money to him to help him unlock tasks, she told Halifax that her partner had been trading currency and paying a “merchant” (rather than his employer). So, even if I were to accept that Halifax ought reasonably to have intervened here and made further enquiries, it seems unlikely that Halifax would've been able to prevent the scam if Miss P had given this same reason, rather than being upfront about the details of the employment scam.
- Halifax also wouldn't have been able to do anything to recover the money Miss P paid from her account either. We know that the money she paid via faster payment was transferred on to her partner and wouldn't have remained in her crypto account. And there wouldn't have been any reasonable prospect of a chargeback claim succeeding for the debit card payments either given Miss P Received and utilised the cryptocurrency she paid for using her Halifax card.

I appreciate this will likely come as a disappointment to Miss P, and I'm sorry to hear about the scam that her and her partner have fallen victim to. However, in these circumstances, I won't be asking Halifax to pay anything over and above the money it has already reimbursed to Miss P.

### **My final decision**

For the reasons given above, I do not uphold this complaint.

Under the rules of the Financial Ombudsman Service, I'm required to ask Miss P to accept or reject my decision before 25 March 2024.

Jack Ferris  
**Ombudsman**