DRN-5422626

## The complaint

Mr A complains that Bank of Scotland plc trading as Halifax didn't do enough to protect him from the financial harm caused by a job scam, or to help him recover the money once he'd reported the scam to it.

## What happened

The detailed background to this complaint is well known to both parties. So, I'll only provide a brief overview of some of the key events here.

On 4 January 2024, Mr A received a WhatsApp message about a job opportunity from someone I'll refer to as "the scammer". When he expressed an interest, the scammer told him about an opportunity to earn money by reviewing films on a platform which I'll refer to as "R". The job required him to pay for tasks using cryptocurrency and at the end of a set of 20-30 'tasks', he would earn commission, and the original deposits would be returned. The scammer told him that a profit was guaranteed.

The scammer told Mr A to open an account with a cryptocurrency exchange which I'll refer to as K and to first purchase cryptocurrency and then load it onto an online wallet. Between 9 January 2024 and 29 March 2024, Mr A made nine transfers from Bank H to K totalling £64,278.

In addition to the transactions from Halifax, Mr A also made three transfers from W totalling £3,502, two transfers from Bank L totalling £19,000, two transfers from Bank N totalling £7,749, and one debit card payment and 38 transfers from R.

Having completed the necessary tasks, Mr A asked the scammer if he could make a withdrawal and was told he'd need to make further payments. He realised he'd been scammed on 13 April 2024 when he ran out of money, he lost contact with the scammer and was unable to access his funds.

Mr A complained to Halifax, and it agreed to refund £7,632 with interest and £40 compensation. It said it intervened several times including on 24 January 2024 when Mr A sent £5,947 to K. It said he was told to lie to his banks by the scammer, and he had several opportunities to tell it why he was making the payments, and had he done so it would have uncovered the scam.

However, later the same day, Mr A tried to send £15,364 to his cryptocurrency account. It blocked the account and released the payment after he told it he was sending money to his own account. Halifax said it accepted it should have kept the restrictions in place for 24 hours to give Mr A time to reflect on what he was doing. So, it agreed to refund 50% of the loss from that point onwards.

Mr A wasn't satisfied and so he complained to this service with the assistance of his representative who argued that Mr A had never purchased cryptocurrency or made such frequent payments to new and different recipients and Halifax should have been on the lookout for job/task-based scams. They argued that Halifax should have asked probing

questions and had it done so, it would have identified that Mr A was falling victim to a job scam because he was contacted unexpectedly on WhatsApp which is inconsistent with how genuine job opportunities arise, he was asked to open a cryptocurrency account, added to a WhatsApp group of others doing this same job, and required to make deposits to unlock premium tasks to earn commission. Further, the payments were getting larger and more frequent, which is common in a job scam, and he was encouraged to take out loans or borrow from family or friends, he was put under pressure to make payments, he didn't have an employment contract, and he was told he could double his investment.

The representative said Halifax's questioning on 21 January 2024 was insufficient to uncover the scam because they were irrelevant to the scam type. They said Halifax should have asked specific questions about the purpose of the payments and had it done so the scam would have been exposed.

They explained that Mr A believed the opportunity was genuine because he'd checked R's website and chatted to the agent via WhatsApp. He thought website seemed authentic and he'd heard of it before. He thought the job was genuine because he had no experience in the type of work offered, there had been a lot of media coverage regarding the move to remote work, and he was added to a WhatsApp group with other employees/freelancers.

Our investigator didn't think the complaint should be upheld. He noted that Halifax intervened on 9 January 2024, and Mr A said no one had contacted him and asked him to make the payment. He was asked to attend the branch on 25 January 2024 where he had another conversation with the fraud team regarding the activity on his account. During the call he was given detailed education on cryptocurrency scams which explained in detail how cryptocurrency investments work. He was also asked whether there was anyone helping him make the payments, which he denied.

He also explained that Mr A had a conversation with Bank T on 10 January 2024, and when asked why he was making the payment, he was reluctant to answer the questions. He eventually said he was making this transfer so that he could purchase a product, but said he wasn't sure which product. He also said he wasn't going to purchase cryptocurrency, and no one had encouraged him to make the payment.

Our investigator thought the scam education and warnings provided by Halifax on 25 January 2024 were good, but Mr A gave misleading answers and was reluctant to listen to the scam advice. He noted that Mr A continued making payments from his Halifax account until 30 March 2024, despite the warning he received on 25 January. He also made two payments from Bank L on 26 January, a day after scam education and warnings from Halifax, as well as payments from R between 1 and 14 February 2024. Overall, he was satisfied that Halifax did enough, and he didn't think further intervention would have made a difference. So, he thought Halifax's offer was fair.

Finally, he noted that Mr A had transferred funds to a legitimate cryptocurrency exchange in his own name and from there he had purchased crypto and moved it onto a wallet address of their choosing, so there would not have been any funds to recover. And he didn't think he was entitled to any compensation.

Mr A has asked for his complaint to be reviewed by an Ombudsman. His representative has argued that Halifax failed to ask open questions, using its knowledge of scam types and holding his answers up to a reasonable level of scrutiny. They've also said the warnings were insufficient because they were only relevant to cryptocurrency investment scams and Halifax ought to know that cryptocurrency investment scams are not the only scam type involving cryptocurrency. They've said that Halifax didn't ask what Mr A was using the cryptocurrency for and merely assumed that he was purchasing cryptocurrency as an

investment. And the warnings didn't resonate with him because they weren't relevant to his circumstances.

The representative has also suggested that our investigator's view contradicts the approach of this Service that banks and EMIs are expected to be on alert for job/task-based scams and taking measures to detect and warn about them. They disagree that Mr A should have disclosed that he was sending money to receive commission from an online job and have argued that Halifax should have given him a job/task scam warning as it knew he was purchasing cryptocurrency.

They've argued that Halifax should have asked Mr A why he was making the payment, and that the call handler jumped to the conclusion that he was using the funds for an investment, which led to ineffective warning. They have also argued that Mr A displayed a significant lack of knowledge about cryptocurrency because he forgot the names of the cryptocurrency wallets he was using, and it failed to question why he was using numerous different wallets or what research he'd done.

**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've reached the same conclusion as our investigator. And for largely the same reasons. I'm sorry to hear that Mr A has been the victim of a cruel scam. I know he feels strongly about this complaint, and this will come as a disappointment to him, so I'll explain why.

I'm satisfied Mr A 'authorised' the payments for the purposes of the of the Payment Services Regulations 2017 ('the Regulations'), in force at the time. So, although he didn't intend the money to go to scammers, under the Regulations, and under the terms and conditions of his bank account, Mr A is presumed liable for the loss in the first instance.

There's no dispute that this was a scam, but although Mr A didn't intend his money to go to scammers, he did authorise the disputed payments. Halifax is expected to process payments and withdrawals that a customer authorises it to make, but where the customer has been the victim of a scam, it may sometimes be fair and reasonable for the bank to reimburse them even though they authorised the payment.

*Prevention*

I've thought about whether Halifax could have done more to prevent the scam from occurring altogether. Buying cryptocurrency is a legitimate activity and from the evidence I've seen, the payments were made to a genuine cryptocurrency exchange company. However, Halifax ought to fairly and reasonably be alert to fraud and scams and these payments were part of a wider scam, so I need to consider whether it did enough to warn Mr A when he tried to make the payments. If there are unusual or suspicious payments on an account, I'd expect Halifax to intervene with a view to protecting Mr A from financial harm due to fraud.

Halifax has agreed to a partial refund, so I need to consider whether the offer is fair. The first three transactions were low value payments to Mr A's own account with another bank, and even though they occurred on the same day, I don't think Halifax needed to intervene.

I've listened to the calls that took place on 9 January 2024, 21 January 2024, and 24 January 2024, and I don't think better questioning would have uncovered the scam because Mr A wasn't honest about why he was making the payments when it questioned him more

thoroughly on 25 January 2024, or when his other banks intervened. So, Halifax wouldn't have detected the scam.

Mr A's representative has argued that Halifax just assumed that he was using the funds for an investment, but I'm satisfied that Mr A said he was buying cryptocurrency for investment purposes. They have also argued that even if he didn't disclose information to suggest he was the victim of a job scam, Halifax should have warned him about job scams because they are so common. But I don't think it's reasonable to expect banks to give warnings about scam types that they don't reasonably suspect are happening. And I don't think a warning about job scams would have made any difference because he made further payments to the scam after having received warnings from his other banks, and he clearly trusted that the job was genuine to the extent that he was prepared to mislead his banks in order for the payments to be processed. I also note that he was given a detailed warning about cryptocurrency investment scams before he went ahead with payments five and six (which Halifax has agreed to refund). So, I don't think Halifax could have stopped the scam before the first payment it has agreed to refund, therefore I'm satisfied its offer is fair.

*Recovery*

I've thought about whether Halifax could have done more to recover the card payments when he reported the scam to it. Chargeback is a voluntary scheme run by Visa whereby it will ultimately arbitrate on a dispute between the merchant and customer if it cannot be resolved between them after two 'presentments'. Such arbitration is subject to the rules of the scheme — so there are limited grounds on which a chargeback can succeed. Our role in such cases is not to second-guess Visa's arbitration decision or scheme rules, but to determine whether the regulated card issuer (i.e. Halifax) acted fairly and reasonably when presenting (or choosing not to present) a chargeback on behalf of its cardholder (Mr A).

Mr A's own testimony supports that he used cryptocurrency exchange to facilitate the transfers. It's only possible to make a chargeback claim to the merchant that received the disputed payments. It's most likely that the cryptocurrency exchanges would have been able to evidence they'd done what was asked of them. That is, in exchange for Mr A's payments, they converted and sent an amount of cryptocurrency to the wallet address provided. So, any chargeback was destined fail, therefore I'm satisfied that Halifax's decision not to raise a chargeback request the cryptocurrency exchange company was fair.

And I don't think there was a realistic prospect of a successful recovery because Mr A paid an account in his own name and moved the funds onwards from there.

*Compensation*

The main cause for the upset was the scammer who persuaded Mr A to part with his funds. I haven't found any errors or delays to Halifax's investigation, so I don't think he is entitled to any compensation.

Overall, I'm satisfied Halifax took the correct steps prior to the funds being released – as well as the steps it took after being notified of the potential fraud. I'm sorry to hear Mr A has lost money and the effect this has had on him. But for the reasons I've explained, I don't think Halifax is to blame for this and so I can't fairly tell it to do anything further to resolve this complaint.

**My final decision**

For the reasons I've outlined above, my final decision is that I don't uphold this complaint.

Under the rules of the Financial Ombudsman Service, I'm required to ask Mr A to accept or reject my decision before 12 September 2025.

Carolyn Bonnell
**Ombudsman**