

The complaint

Mr C complains that Bank of Scotland plc trading as Halifax didn't do enough to prevent him falling victim to an advance fee job scam.

Mr C has used a representative to bring his complaint. But, for ease of reading, I'll mostly just refer to Mr C throughout my decision where I also mean the representative.

What happened

The detailed background to this complaint is well known to both parties. So, I'll only provide an overview of some of the key points here. In 2023 Mr C says he was the victim of a job scam. He received a message about an opportunity for remote work. Mr C responded to the message and learned that the job was 'optimising applications' by completing tasks after which he would be paid a commission. He was also told there were 'premier tasks' which meant he had to make a payment first but would then see a larger commission. He was added to a group chat which included others who were sharing their success with the same scheme.

Mr C says that as a result of the scam, he made the below payments. All these payments went to F, which is a cryptocurrency exchange that he'd been using since 2021. I understand the purchased cryptocurrency was then sent on to the scammers and lost. It is also relevant that shortly before this scam, Mr C was the victim of a separate investment scam. This involved him making two payments (each of £2,500) on 19 September 2023. These payments also went through F. Those payments are being dealt with separately in Mr C's linked complaint.

Payment Number	Date	Amount
1	17 October 2023	£20
2	17 October 2023	£1,380
3	18 October 2023	£3,000
4	18 October 2023	£1,255
5	19 October 2023	£4,270
6	19 October 2023	£3,000
7	19 October 2023	£2,720

Mr C says that he then realised that if the pattern continued, that he would never receive any money and concluded he'd been victimised again.

In November 2023, Mr C complained to Halifax that they hadn't done enough to protect him from the scam. Halifax responded to the complaint but didn't offer any redress. They pointed out that they had warned Mr C about job scams prior to him making his final payment. Mr C referred his complaint to our service and one of our Investigators didn't recommend that it should be upheld. He wasn't persuaded that Halifax were responsible for the loss. Mr C disagrees and has asked for an Ombudsman to review his complaint.

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 outcome as our Investigator and for similar reasons. I know this will be disappointing for Mr C, so I'll explain why.

Halifax's first obligation is to follow the payment instructions from their customers like Mr C. And it isn't in dispute that Mr C himself instructed the payments relevant to this complaint. So the starting position is that Mr C is usually responsible for payments he's instructed himself. But that isn't the end of the story. Halifax should also be alert to the potential for fraud, scams and the misappropriation of funds. And they should do what they can to protect their customers from these risks.

I think it was appropriate for Halifax to block some payments and to speak with Mr C prior to processing his last payment towards the scam. It's arguable that this intervention also ought to have taken place sooner than it did, given the increase in the velocity and value of the payments being made to F (who Halifax would've known or likely could've ascertained was a cryptocurrency exchange). But at whichever point it should've happened, for the reasons I'll come to, I don't think it would've resulted in Mr C ending up in a meaningfully different position.

During the call I've listened to, the agent asks whether Mr C is sending the money in advance to receive a return, he confirms that he isn't. The agent asks which cryptocurrencies Mr C is buying and he answers, mentioning specific assets. The agent also confirms that Mr C is doing all this himself and that no-one else has access to Mr C's account with F. It is also explained that a bank transfer is like cash and if this is a scam, Mr C would lose his money. Later in the same call the following exchange takes place between Mr C and Halifax's agent.

Halifax: *"At the moment what we're seeing is an increase in the job MO online. So customers come across a job online, and they apply for the job. They're asked to complete daily tasks. When they complete these tasks they are given commission. They're commission is shown in an account, but to withdraw their commission, they're asked to make a payment to the fraudsters with cryptocurrency. So, can I just confirm with you as well that, you know, you have not come across a job online and you're not paying money through cryptocurrency to get your commission released, is that right?"*

Mr C: *"Yeah, yeah, nothing like this."*

Mr C then goes on to make his further payment whilst still on the call with Halifax's agent.

I think Halifax's warning was appropriate and it closely matched the scam that Mr C was a victim of.

When our Investigator asked Mr C, he also said that he hadn't been coached by the scammer as to how to answer any questions from his bank if challenged. With that in mind, I'm not sure why he told Halifax's agent that he was just buying cryptocurrency under his own direction, rather than sharing the situation as he now describes it, which is that the payment was connected to a job scam, where he'd been completing tasks to earn commission.

I think the intervention and warnings by Halifax were appropriate and they specifically warned Mr C about the scam that he was a victim of. I don't think Halifax reasonably could've known or uncovered that Mr C wasn't being truthful with them in his responses. And this warning wasn't impactful in stopping payments (as Mr C made his final payment after it had been given). So even if this warning should've come sooner, I think things would've turned out largely as they did, which is that it wouldn't have stopped further payments from Mr C.

I've noted Mr C's point that Halifax should've been more cautious as he'd recently been a victim of a scam involving him paying the same payee. But I still think the intervention from Halifax was sufficient in these circumstances. Similarly Mr C has said he was vulnerable at the time in part due to a close family member being very unwell. I'm sorry to hear of Mr C's personal circumstances. But I've not seen evidence to support that Halifax was made aware of this situation and I don't think it's something I fairly could've expected them to have ascertained themselves. So it isn't a basis upon which I could expect them to have done more.

For completeness, I'm also satisfied that the Lending Standards Board's Contingent Reimbursement Model (CRM Code) doesn't apply in this case. This was a scheme through which victims of scams could sometimes receive redress from the banks involved. But it required that any payments were made to another person, and here, the payments went to Mr C's own account with F.

I've gone on to think about whether Halifax could've done more to help recover the same, once aware of the problem. But in the circumstances here, Mr C's testimony is that the payments were exchanged for cryptocurrency which was sent on to the scammers. So I don't think anything Halifax did or didn't do at that point would've impacted whether a recovery could've been made.

Again, I'm sorry to hear Mr C lost the money he did, but as I don't think this is something Halifax can fairly be said to be responsible for, there isn't a reasonable basis upon which I can require them to do more to resolve this complaint.

My final decision

For the reasons 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 C to accept or reject my decision before 18 August 2025.

Richard Annandale
Ombudsman