DRN-4478361

The complaint

Mr N complains Bank of Scotland plc trading as Halifax didn't do enough to protect him when he fell victim to a scam and won't refund the £3,750 he lost as a result.

What happened

Mr N fell victim to a task-based employment scam in July 2023. He was contacted by someone purporting to be from a legitimate recruitment agency ("the scammer"), who offered him part-time work, which he could complete remotely. The scammer told him he would be paid in crypto for completing online tasks to help an American advertising company ("IV") *"generate real data"*. Upon completion of certain sets of tasks, Mr N was told he would receive commission.

The scammer instructed Mr N to set up a working account with IV (although this was in fact a clone of the legitimate company's website), where he would complete his tasks. Mr N was also instructed to open an account with, and transfer money to, an FCA-authorised Electronic Money Institute ('EMI'). He was also told to set up a crypto account with a legitimate crypto exchange platform, where he would receive his earnings but could also top up his working account to reset his tasks. Mr N explained that he initially used crypto the scammers had provided him with. But, having completed certain promotional tasks which generated higher commissions but were themselves increasingly expensive, the account fell into a negative balance, and he needed to top up the account with further crypto purchases. Mr N initially purchased crypto via his EMI account, but later started making payments from his Halifax account.

Mr N made the following payments from his Halifax current account:

Date	Payment type	Amount
21/07/23	Faster Payment	£2,000 (reverted)
24/07/23	Faster Payment	£1,000
24/07/23	Faster Payment	£2,750
	Total loss	£3,750

The payments were made to a third party, unconnected to the scam, as Mr N had purchased crypto via a peer to peer (P2P) service provided by the crypto exchange. Mr N then transferred the crypto from his wallet into his working account with IV, at which point it was in the control of the scammer.

Before processing the first and second payments, Halifax contacted Mr N by telephone and asked him about the purpose of the payments and provided him with broad crypto warnings. Mr N acknowledged the warnings and decided to continue with the payments.

The first attempted payment was returned to Mr N's account by the merchant on the same day, so did not add to his loss.

Mr N said he realised he'd been scammed when the website for IV suddenly went offline. He attempted to contact the scammers but was told he needed to top up his account. He reported the scam to Halifax and asked it to reimburse his losses.

Halifax attempted to recover the payments but was unsuccessful as the beneficiary bank confirmed that no funds remained. It declined to refund any of the payments Mr N had lost to the scam as it said he had properly authorised them. It also said he had failed to take reasonable steps to protect himself from the scam – for example checking if the person he was speaking with was legitimate and questioning why he had to pay money for work he expected to receive payment for.

Unhappy with Halifax's response, Mr N referred his complaint to the Financial Ombudsman. He said Halifax should have done more to warn him about the risks associated with job scams. He suggested that it was therefore liable for his loss.

Our Investigator didn't uphold the complaint. She was satisfied that Halifax had intervened as we would have expected it to but given Mr N's responses to the questions, it was unable to uncover the scam or prevent Mr N's loss.

Mr N disagreed and asked for an Ombudsman's final decision. He felt the Investigator had misunderstood the facts of the complaint, which had influenced the outcome she reached. He also maintained that the answers he gave to Halifax's questions were accurate. He considered that Halifax ought to have stopped his transactions when it realised he was buying crypto.

So, the case has been passed to me to decide.

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'm not upholding this complaint and for largely the same reasons as our Investigator. I realise this will come as a disappointment to Mr N, but for the reasons I'll go on to explain I don't think Halifax has acted unfairly.

I'm sorry to hear Mr N was the victim of a sophisticated and targeted scam and lost a significant sum of money as a result. I can appreciate why he wants to do all he can to recover the money he lost. But I can only direct Halifax to refund Mr N's losses if it can fairly and reasonably be held responsible for them.

It is evident that Mr N authorised each of the scam payments from his Halifax account. So, although he didn't intend the money to go to the scammers, under the Payment Services Regulations 2017 and the terms and conditions of his account, Mr N is presumed liable for his loss in the first instance. And under the terms and conditions of the account, where a valid payment instruction has been received, Halifax's obligation is to follow the instructions Mr N provides.

For clarity, I should explain that the Contingent Reimbursement Model ('CRM') - a voluntary scheme that provides increased protection for victims of authorised push payment scams - doesn't apply in these circumstances, as Mr N's payment went towards the legitimate purchase of crypto, which was only later transferred to the scammer as part of the scam.

While the CRM doesn't apply, there are other regulatory expectations and requirements and what I consider to have been good industry practice at the time, that meant Halifax should

fairly and reasonably have been on the look-out for the possibility of fraud and have taken additional steps, or made additional checks, before processing payments in some circumstances.

Whilst I have set out in detail the circumstances which led Mr N to make payments using his Halifax account and the process by which that money ultimately fell into the hands of the scammer, I am mindful that Halifax had much less information available to it upon which to determine whether any of the payments presented an increased risk that Mr N might be the victim of a scam.

Nevertheless, Halifax did carry out further checks before processing Mr N's first two payments. On both occasions Halifax fraud prevention agents spoke to Mr N to ask for further information about the payments he was making.

In the first call, Mr N said he was purchasing crypto to buy goods and services. He said he'd used the company before, having made payments through his EMI account. He was now using his Halifax account as he had funds available. He said his crypto was then changed for dollars for what he was doing. He said he had found out about the opportunity through friends. He advised that no one had approached him to get him involved and no one had asked him to open an account. When asked about the research he had carried out Mr N commented "*this is my money isn't it. I'm taking the risk at doing this today*." Halifax gave Mr N a broad warning about the risk of crypto transactions and asked him to confirm that he hadn't been contacted by anybody else or told to lie to the bank or been asked to make the payment for any reason other than he had stated. Mr N replied *"no".*

In the second call, Mr N again said he was purchasing crypto to buy goods. When probed about the reason for the payment Mr N commented *"it's definitely not a scam I went through all this yesterday."* He went on to confirm he had set up the account himself. Halifax's fraud prevention agent advised that there were lots of crypto scams which always involved a third party in the background - *"someone pretending to be an account manager or investor so someone that can make you money quickly",* which Mr N acknowledged. Mr N denied being sent links or portals to click on to do the transfer. Mr N was again given a warning about the risk of crypto transactions and advised that if he made the payments and it turned out to be a scam it was unlikely the money could be recovered.

Having reviewed both calls, I think Halifax could potentially have asked further questions to understand the nature of Mr N's payments, as his answers had been vague. But overall, I consider Halifax's intervention was proportionate to the risks it had identified. While it understood that Mr N was buying crypto, it was reassured by the fact that this was an existing relationship and Mr N had said he'd become aware of the opportunity through friends. The payments were also relatively modest and in line with Mr N's usual account usage. There were also no other clear flags or patterns to suggest the payments were linked to a scam.

I must also factor in that Halifax could only tailor its warnings to the information Mr N provided. While Mr N was not wholly dishonest when answering Halifax's questions, I don't think he was as forthcoming with information as he could have been, and this limited Halifax's ability to understand what was really going on. Had Mr N revealed that he had been contacted by a recruiter on a social media platform, I think this would have given Halifax more cause for concern and would have given it reason to question him further. I think he could also have revealed that his payments were linked to employment and that he had been asked to set up various accounts.

While task-based employment scams are becoming increasingly prevalent, at the time Mr N made his payments (July 2023) I would not have expected Halifax to specifically ask him

questions related to task-based employment scams, and I don't think any of the answers Mr N gave to Halifax's questions ought to have given it reason to believe that was the scam he was falling victim to.

But even if Halifax could have done more, I must also decide whether any further intervention would have made a difference to Mr N's decision to make the payments, and I don't think it would. In both conversations, Mr N demonstrated an awareness of the risk of scams but made clear he was prepared to accept the risk with his money.

I've considered whether, on being alerted to the scam, Halifax did enough to recover Mr N's losses. I can see that Halifax did attempt to recover the lost funds, but it was confirmed by the beneficiary banks that no funds remained. But even if funds had remained Mr N would not have been entitled to reimbursement as there is no dispute that Mr N received the crypto he paid for. His loss only occurred when he transferred the crypto into the control of the scammers.

In conclusion, I have a great deal of sympathy with Mr N being the victim of what was clearly a cruel scam. But it would only be fair for me to direct Halifax to refund his loss if I thought it was responsible – and I'm not persuaded that this was the case. Everything considered, I cannot fairly and reasonably hold Halifax liable in these circumstances. It follows that I will not be asking it to take any further action.

My final decision

For the reasons given above, my final decision is that I do not uphold this complaint.

Under the rules of the Financial Ombudsman Service, I'm required to ask Mr N to accept or reject my decision before 17 April 2024.

Lisa De Noronha
Ombudsman