DRN-4625292

The complaint

Mr N has complained that Bank of Scotland Plc (trading as "Halifax") failed to protect him from falling victim to an investment scam.

What happened

The background of this complaint is already known to both parties, so I won't repeat all of it here. But I'll summarise the key points and then focus on explaining the reason for my decision.

Mr N has used a professional representative to refer his complaint to this service. For the purposes of my decision, I'll refer directly to Mr N, but I'd like to reassure Mr N and his representative that I've considered everything both parties have said.

Mr N says that in July 2023 he was actively seeking a job when he received an unsolicited message via from an individual on a messaging app, posing as a recruiter. The scammer claimed that Mr N had shown interest in one of the roles they had available, so Mr N was contacted on another messaging app by another individual ("the scammer") who provided further details about the opportunity. She described the role as involving brand boosting and marketing for a legitimate company. Mr N says the opportunity seemed credible, given the company's established reputation, so he was keen to learn more.

The job required Mr N to complete tasks on an online platform. The tasks involved simulating the purchase of various items, such as hair dryers and washing machines. Mr N was told that merchants benefited from these simulated purchases because it improved their product algorithms, increasing the likelihood of sales. To participate, Mr N was required to deposit money into the platform, which would be used to simulate the purchases. For each task completed, he was promised a commission, and after completing a set of tasks, he would supposedly be able to withdraw both his initial deposits and the commission he'd earned. In order to deposit money into the work platform Mr N was required to add funds to his wallet at a cryptocurrency exchange, and purchase cryptocurrency. He did this in two ways; by using his debit card to top up his balance at the cryptocurrency platform, and also by making payments (bank transfers) to his wallet at the cryptocurrency platform. He then transferred the cryptocurrency to a wallet directed by the scammer, under the illusion he was funding his work account.

At first, the arrangement appeared legitimate. Mr N was able to complete up to 39 tasks twice daily, earning commission of up to £100 per day. He says he received an initial return of £66.10, which was paid into his Halifax account. He was added to a group chat with other "freelancers," who shared their successes and daily activities, and a mentor provided one-on-one training to guide him through the process. These elements gave Mr N confidence in the opportunity.

To further verify the legitimacy of the job, Mr N says he carried out several checks. He searched online and found positive reviews of the platform and the associated company. He also says he checked on a professional networking site and found the company was a genuine business. Having posted his CV on various job search platforms, Mr N says he

didn't find it unusual to be contacted with a job offer, especially one presented in such a professional manner.

As Mr N continued to complete tasks, the deposits required for each task increased. Towards the end of the process he was asked to make a significant additional payment of 6630 USDT (a cryptocurrency). At this point, Mr N began to suspect something was wrong. The scammer started responding with automated messages, and he noticed that no formal employment contract or service agreement had been provided.

Mr N made payments and received payments using two different Halifax accounts as follows:

Date	Amount (£)
13/07/2023	32.36
13/07/2023	20.00
14/07/2023	64.06
14/07/2023	64.04
14/07/2023	15.01
17/07/2023	199.67
17/07/2023	47.92
17/07/2023	479.10
17/07/2023	1,600.70
17/07/2023	760.32
17/07/2023	95.95
17/07/2023	79.97
14/08/2023	2,975.40
14/08/2023	500.00
14/08/2023	438.82
18/08/2023	871.70
18/08/2023	802.74
23/08/2023	3,404.63
23/08/2023	1,741.38
23/08/2023	15.00
Total	**14,208.77**

Account 1

Date	Amount (£)	Type
13/07/2023	+198.49	Credit
13/07/2023	+66.10	Credit
14/07/2023	200.00	Debit card
15/07/2023	79.97	Payment
15/07/2023	95.95	Payment
15/07/2023	479.10	Payment
15/07/2023	1,600.70	Payment
15/07/2023	760.32	Payment
13/08/2023	2,975.40	Debit card
13/08/2023	432.82	Debit card
13/08/2023	500.00	Debit card
Total	**7,388.85**	

Account 2

Date	Amount (£)	Type

13/07/2023	20.00	Debit card
13/07/2023	32.26	Debit card
13/07/2023	15.01	Debit card
13/07/2023	60.04	Debit card
13/07/2023	64.06	Debit card
14/07/2023	199.67	Debit card
14/07/2023	47.92	Debit card
17/08/2023	802.74	Debit card
17/08/2023	871.70	Debit card
22/08/2023	15.00	Debit card
22/08/2023	1,741.38	Debit card
22/08/2023	3,404.63	Debit card
Total	**7,274.41**	

When Mr N realised he'd fallen victim to the scam he contacted Halifax to report it. He says Halifax told him it couldn't help him any help further. Although Mr N hasn't yet reported the matter to Action Fraud, he plans to do so.

Mr N says several factors made the scam appear legitimate. The job offer came at a time when he was actively searching for employment, and it was presented as a professional opportunity with a reputable company. The scammers reinforced this perception by creating a structured environment that included a dedicated mentor, initial returns on his investments, and a group chat with other "freelancers" who shared their experiences. He also says the platform itself appeared professional, and online searches revealed positive reviews.

Mr N made a complaint to Halifax on the basis that it failed to identify the warning signs of the scam, and it should've provided better support when he reported it. He says that if it had done more to intervene, the scam would've been uncovered and his losses minimised. Halifax didn't uphold Mr N's complaint. In its response it said that as the payments had been made using Mr N's debit card, they weren't covered by the Contingent Reimbursement Model ("CRM") Code and it therefore declined to refund them. It also said it thought Mr N ought to have done more to protect himself from the scam.

Mr N remained unhappy so he referred the complaint to this service.

Our investigator considered everything and didn't think the complaint should be upheld. She explained that although she thought Halifax should've intervened when Mr N made the payment for £1,600.70 on 15 July 2023, she didn't think it would've been able to uncover the scam as Mr N had given some untruthful information to Halifax about the circumstances of the scam.

As Mr N didn't accept the investigator's opinion, the case has been passed to me to make a decision.

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.

I'm sorry to disappoint Mr N but having considered everything I'm afraid I'm not upholding his complaint, broadly for the same reasons as our investigator, which I've set out below.

In broad terms, the starting position is that a firm is expected to process payments and withdrawals that its customer authorises, in accordance with the Payment Services

Regulations and the terms and conditions of the customer's account. And in this case it's not in question whether Mr N authorised these payments from leaving his account. It's accepted by all parties that Mr N gave the instructions to Halifax and Halifax made the payments in line with those instructions, and in line with the terms and conditions of Mr N's account.

But that doesn't always mean that the business should follow every instruction without asking further questions or intervening to ensure requests coming from their customers are firstly genuine, and secondly won't result in harm.

Mr N initially raised a claim with Halifax that he didn't recognise the five transactions made from account 1 on 15 July 2023. However as they were made to the same retailer that Mr N had previously used, from the same IP address, Halifax concluded they were in fact authorised by Mr N and declined the claim. The payments were then raised as part of the scam claim, whereby Mr N accepted that he made the transactions, but under the false pretences of funding an employment opportunity.

Having considered everything I agree with our investigator that Halifax ought to have intervened when Mr N made the payment for £1,600.70 on 15 July 2023. By the time that payment was made it was the fourth payment on the same day, to the same recipient, which was an identifiable cryptocurrency exchange. The total of the payments was over £2,000 and I therefore think Halifax ought to have realised Mr N might've been at risk of financial harm and intervened to attempt to prevent that. At the time these payments were made, in July 2023, cryptocurrency scams had risen greatly in frequency and it's reasonable to conclude that Halifax had had time to digest this information and the warnings about cryptocurrency, and put mechanisms in place to detect and prevent this type of fraud.

I'm not aware that Halifax intervened when any of the payments were made, nor did it block any of the debit card payments. Although it blocked and reordered Mr N's debit card when he reported the transactions as unrecognised, it didn't take any other proactive steps to prevent further transactions taking place.

Would an intervention have made a difference?

Although I'm satisfied that Halifax should've intervened, even if it had, I'm not persuaded it would've been able to uncover the scam, for a number of reasons.

Mr N initially told Halifax on 15 July 2023 that he didn't recognise the transactions made to the cryptocurrency platform. But this is at odds with the evidence he's provided which shows a chat between Mr N and a scammer before that date – where they discuss deposits made allegedly for Mr N to carry out the work tasks. He also proceeded to make several more transactions to the same payee which indicates he did in fact recognise it.

I've also listened to a call between Mr N and Halifax that took place on 15 November 2023. At that time Mr N told Halifax not only did he not recognise the cryptocurrency transactions, but that he didn't have an account with the cryptocurrency platform the transactions had been made to. But the evidence I've been provided shows that Mr N had held his cryptocurrency wallet for at least a few days before that call took place – and had funded it with several payments.

With these points in mind, even if Halifax had intervened, I'm not persuaded Mr N would've been honest about the purpose of the payments he was making. It's clear there was something in his mind preventing him from telling Halifax the truth, although I don't know what that was. But I'm not persuaded that Mr N would've changed his story or taken a different approach, even if Halifax had asked him further questions about the transactions, either as automated on-screen questions, or as part of a human intervention. So I don't

think an intervention would've made a difference in this case, and consequently I don't hold Halifax responsible for the losses Mr N unfortunately made as part of this scam.

Is Mr N responsible for any of his losses?

I've also thought about whether Mr N did enough to satisfy himself that the job opportunity he was allegedly sending money to take part in was genuine and wouldn't result in him losing that money.

I accept that Mr N has fallen victim to a carefully crafted scam here, and Mr N has provided screenshots of the work platform he was given access to, which I understand appeared convincing to him.

But it's very unusual for a recruiter to contact a prospective candidate out of the blue, and offer them a job through a messaging app, without having ever spoken to them. I'm also not aware that Mr N did any checks to verify the recruiter or the job opportunity, nor received any kind of paperwork or employment contract showing what he thought he'd been offered, or what he'd agreed to do in return. This, as well as having to pay in cryptocurrency to earn money in return, isn't a plausible scenario.

Recovery of the funds

In this case Mr N made the payments to a cryptocurrency wallet in his own name, and he then used the funds to purchase cryptocurrency which he sent to the scammer.

As Mr N purchased cryptocurrency, he'd effectively spent the funds, so recovery wouldn't have been an option to Halifax. In addition, any remaining funds that Mr N hadn't converted into cryptocurrency would've remained in his cryptocurrency wallet, under his control, so they wouldn't have formed part of the loss attributable to the scam.

I've seen Mr N's representative's point that Mr N was confused about the payments he said he didn't recognise, and that this doesn't mean Halifax wouldn't have been able to uncover the scam with further questioning. But I have to make my decision on what I think is most likely to have happened – and in this case the evidence persuades me it's more likely than not that Mr N wouldn't have been truthful with Halifax if it had intervened to ask for further details about the payments that were part of this scam.

I'm very sorry that Mr N has fallen victim to this scam and I do understand that my decision will be disappointing. But for the reasons I've set out above, I don't hold Halifax responsible for that.

My final decision

I don't uphold Mr N's complaint against Bank of Scotland Plc, trading as Halifax.

Under the rules of the Financial Ombudsman Service, I'm required to ask Mr N to accept or reject my decision before 30 January 2025.

Sam Wade
Ombudsman