DRN-5819689

The complaint

Mr F complains that Bank of Scotland plc, trading as Halifax, won't refund the money he lost to a job scam.

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.

In April 2025, Mr F received a message on his messaging app offering him a job opportunity. The job was on-line earning commission for completing simple reviews, which appear to have been aimed at boosting search engine optimisation.

Mr F accepted the job and received training. He was assigned a mentor, and an account was created for him on a fake company platform.

After completing sets of tasks and earning some commission, higher earning tasks became available. But these created a negative balance on his fake account. Mr F was required to pay the fake company in crypto from his crypto account, which he already had with Company C (a legitimate crypto exchange).

To be able to both continue with the job and withdraw funds Mr F found it necessary to pay back the commission he earned and then add more money. Mr F made the following payments to Company C from his Halifax account:

Payment Number	Date	Payment method	Payee	Amount
1	15/4/25	Debit card	Mr F's account with Company C	£78.80
2	16/4/25	Debit card	Mr F's account with Company C	£62.16
3	18/4/25	Debit card	Mr F's account with Company C	£1,948.02
4	18/4/25	Debit card	Mr F's account with Company C	£1,121.73
5	18/4/25	Debit card	Mr F's account with Company C	£2,885.29
Total				£6,096.00

Mr F became suspicious and stopped paying the scammers when he was told to make a large payment. Also, Halifax stopped further payments.

Mr F contacted Halifax about how he could obtain a refund. He was initially misadvised as he was told to call back as some payments were still pending, giving him the wrong impression some of his loss could be prevented. Also, they told him to contact Company C.

After escalating his complaint to our service, Halifax said they should've intervened upon payment five and awarded him a refund of 50% of this payment as they considered he was partly liable for the losses. Also, they awarded him £60 (increased from £30) for the trouble and upset caused by the misinformation given to him about recovering his funds.

Mr F was dissatisfied with this, but our investigator considered Halifax's offers to have been fair and reasonable.

Mr F remained dissatisfied and asked for an ombudsman to look at his complaint. Also, he provided information on his learning disability.

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, although I'm very sorry to hear that Mr F has been the victim of this cruel scam and lost a significant amount of money here, I'm not upholding this complaint. And I'll explain why.

I should first say that:

- In making my findings, I must consider the evidence that is available to me and use it to decide what I consider is more likely than not to have happened, on balance of probabilities.
- I'm satisfied that the APP Scam Reimbursement Rules, introduced by the Payment Systems Regulator in October 2024, for customers who have fallen victim to an APP scam, don't apply here as the payments were made by card.
- Regarding efforts to recover Mr F's loss. As the payments to the scammer were sent to a crypto exchange and then onto the scammer, I don't think Halifax could've been expected to recover them. Also, as explained by our investigator, unfortunately it wouldn't have been possible for Halifax to raise a card chargeback claim as the rules don't cover scams.
- The Payment Services Regulations 2017 (PSR) and Consumer Duty is relevant here.

  PSR

  Under the PSR and in accordance with general banking terms and conditions, banks should execute an authorised payment instruction without undue delay. The starting position is that liability for an authorised payment rests with the payer, even where they are duped into making that payment. There's no dispute that Mr F made the payments here, so they are considered authorised.

  However, in accordance with the law, regulations and good industry practice, a bank should be on the look-out for and protect its customers against the risk of fraud and scams so far as is reasonably possible. If it fails to act on information which ought reasonably to alert a prudent banker to potential fraud or financial crime, it might be liable for losses incurred by its customer as a result.

  Banks do have to strike a balance between the extent to which they intervene in payments to try and prevent fraud and/or financial harm, against the risk of unnecessarily inconveniencing or delaying legitimate transactions. So, I consider Halifax should fairly and reasonably:

  - Have been monitoring accounts and any payments made or received to counter various risks such as anti-money laundering and preventing fraud and scams.
  - Have systems in place to look out for unusual transactions or other signs that might indicate that its customers were at risk of fraud (among other things). This is particularly so given the increase in sophisticated fraud and scams in recent years, which banks are generally more familiar with than the average customer.

- In some circumstances, irrespective of the payment channel used, have taken additional steps, or made additional checks, before processing a payment, or in some cases declined to make a payment altogether, to help protect customers from the possibility of financial harm from fraud.

Consumer Duty

Also, from July 2023 Halifax had to comply with the Financial Conduct Authority's Consumer Duty which required financial services firms to act to deliver good outcomes for their customers. Whilst the Consumer Duty does not mean that customers will always be protected from bad outcomes, Halifax was required to act to avoid foreseeable harm by, for example, operating adequate systems to detect and prevent fraud. Also, look for signs of vulnerability.

Halifax accept they should've done more here. Upon reflection they think they should've put in place a human intervention at payment 5 and give a refund from this point. But Mr F thinks they should provide him with a greater refund.

I first requested information from Mr F about his vulnerabilities. Also, whether he, a power of attorney or family member with a mandate had requested necessary support and assistance from Halifax. In addition, I asked Halifax if they had any records on Mr F's vulnerabilities.

Mr F provided evidence that he had a learning disability when he was an adolescent. This was twelve years ago and without more current information, it is difficult to know the severity level, impact of any therapy he received and whether this is mild or severe. Also, what support arrangements were implemented and remain. However, from this, I'm satisfied he has a vulnerability and that this likely made him more susceptible to this type of scam.

However, neither Mr F or Halifax had any information or records of this, or any other vulnerability being discussed or identified in the approximate ten years that he held the account. And this was despite Mr F having previously made payments to three different crypto companies.

So, although I'm satisfied Mr F likely has a vulnerability as defined by the FCA, as Halifax didn't have any information on this, I wouldn't have expected them to have put in place an exceptional intervention because Mr F was trading in high risk crypto.

Regarding payments 1,2 and 3, that Halifax would've known were going to crypto, I wouldn't have expected Halifax to have put in place any intervention on these. This is because:

- Company C was an established payee.
- Mr F had also previously made crypto payments to two other crypto companies.
- The amounts were low. Payment 3 was the highest of the three payments but not significantly higher than a payment Mr F had made to another crypto company.
- Crypto payments are common and aren't illegal and banks like Halifax process thousands of payments each day and as mentioned above have a careful balance to strike when considering intervention as they shouldn't unnecessarily inconvenience or delay legitimate transactions.

Regarding payment 4, as this was the second payment on 18 April 2024 (bringing the spend at that point to just over £3,000), even though Mr F wasn't new to crypto, I would've expected to have seen a written warning about the heightened risks of crypto including fraud and scams.

Although I can't see that Halifax provided this type of warning, importantly, I wouldn't have expected it to contain information on job scams. I think the warnings would've likely been about the risks of dealing with crypto and making investments. So, I don't think this type of warning would've resonated with Mr F.

Also, whilst I recognise Mr F's vulnerability, and Halifax's lack of awareness of this, on balance of probabilities, I think Mr F had likely already been provided with such a warning. I say this because on three occasions he set up new payees for crypto accounts and there is a file note showing a fraud and scam educational message was sent to Mr F prior to a crypto payment he made to Company C, a few months prior to the scam, in November 2024.

Regarding payment 5, Halifax don't dispute that they should've intervened at this point as both the amount, and combined amount, were unusual and outside of Mr F's normal spending pattern. And I agree with their finding that they should've intervened and that a refund is warranted on this payment.

I then considered if it was reasonable for Halifax to deduct 50%.

There's a general principle that consumers must take responsibility for their decisions. Although I recognise how convincing these cruel scammers are and don't at all blame Mr F for paying them, I think he should've done more to protect himself here.

As mentioned above, it is difficult to know the severity level of Mr F's disability. However, I think Mr F ought reasonably to have put in place mitigation for his vulnerability. So, I think he and / or his support (if necessary) ought to have had concerns about being offered a job which appears to neither have had a process or contract. Also, making payments to an employer to undertake work and seemingly earning high commission for basic tasks. In addition, requiring the payment in an unusual and high-risk form (crypto) where he would've likely seen warnings about the prevalence of fraud and scams.

So, although I recognise Mr F has a vulnerability, I think both parties made errors here. I therefore consider Halifax's offer, to equally split liability on the payment that should've been stopped (payment 6 for £2,885.29), to be both fair and reasonable.

Finally, I considered whether Halifax's £60 payment for giving Mr F incorrect information was fair and reasonable. As there wasn't a way of Halifax stopping the pending payments, I can understand Mr F's frustration at being given false hope that some of his loss could be prevented. However, when considering this was an isolated error, there was no way of recovering the funds, the timing of Halifax's apology and that the main distress and inconvenience here was caused by the cruel scammers, I think Halifax's payment is within the compensation range recommended in our publicly available compensation guidance.

So, having considered the above, I'm sorry to disappoint Mr F but my final decision is that I'm not upholding this complaint and requiring Halifax to make any further compensation or refund payments.

My final decision

For the reasons mentioned above, my final decision is that I'm not upholding this complaint against Bank of Scotland plc trading as Halifax.

Under the rules of the Financial Ombudsman Service, I'm required to ask Mr F to accept or reject my decision before 2 January 2026.

Paul Douglas
Ombudsman