

The complaint

Mr K is unhappy Bank of Scotland plc, trading as Halifax, will not refund the money he lost as the result of an authorised push payment (APP) scam.

Mr K brought his complaint through a representative, for ease of reading I will refer solely to Mr K in this decision.

What happened

As both parties are aware of the details of the scam, I will not repeat them in full here. In summary, Mr K fell victim to a job/task scam. He was contacted via WhatsApp and offered the opportunity to complete tasks (optimising apps for a software company) to earn commission. He was told that to access the tasks he first needed to open a digital wallet at cryptocurrency exchange ('K') and then send the funds on to the company's account (the scammer). He made the following faster payments to his digital wallet at 'K':

payment	date	value
1	22/07/2023	£10
2	28/07/2023	£2,500
3	28/07/2023	£2,650
4	07/08/2023	£5,000

Halifax intervened at the time of payment 3. Mr K did not answer its questions honestly and the payment went ahead.

Mr K realised he'd been scammed when he was unable to withdraw his commissions and was given different explanations. He says Halifax did not do enough to protect his money and must refund the payments. The scam was not reported to Halifax until November 2024.

Halifax says the payments are not covered by the CRM (Contingent Reimbursement Model) code as they were to an account in Mr K's name. Based on the answers Mr K gave at the time of payment 3 it had no further concerns and so processed the payment. Mr K had authorised all four payments and it is not liable for his loss.

Our investigator did not uphold Mr K's complaint. She said Halifax intervened at the appropriate point, but Mr K's answers prevented it from identifying the hallmarks of a job/task scam and giving the right warning and support.

Mr K disagreed with this assessment and asked for an ombudsman's review. He said, in summary, as there were entries about 'K' on the IOSCO (International Organisation of Securities Commission) register from July 2022 onwards Halifax should have stopped all his transactions.

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.

In broad terms, the starting position at law is that a bank is expected to process payments and withdrawals that a customer authorises it to make, in accordance with the Payment Services Regulations (in this case the 2017 regulations) and the terms and conditions of the customer's account. It is not in dispute here that Mr K authorised these payments.

But, taking into account relevant law, regulators rules and guidance, relevant codes of practice and what I consider to have been good industry practice at the time, I consider it fair and reasonable that by July 2023 Halifax should:

- have been monitoring accounts and any payments made or received to counter various risks, including preventing fraud and scams;
- have had 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 firms 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, or provided additional warnings, before processing a payment;
- have been mindful of – among other things – common scam scenarios, how the fraudulent practices are evolving and the different risks these can present to consumers, when deciding whether to intervene.

As the scam was reported more than 12 months after the payments were made Halifax no longer has the records showing what, if any, warnings were displayed, whether Mr K was asked for the reason for the payment or any Confirmation of Payee results.

Based on the available evidence however we do know that Halifax identified payment three as higher risk and so spoke with Mr K before processing it. I think this was the right point of intervention given the cumulative spend by Mr K at an identifiable cryptocurrency exchange in one day. Banks need to strike a balance between the extent to which they intervene in payments and unduly inconveniencing or delaying legitimate payment requests. In the contact of Mr K's account history the first two payments did not show the typical characteristics of likely financial harm.

And I don't agree that as 'K' was on the IOSCO register all payments should have been blocked. The entries on the register at this time flagged that 'K' did not have the necessary permissions to trade in certain territories, but these did not include the UK. So, I do not find that Halifax ought to have interpreted the warning to mean it needed to block all payments to 'K'. 'K' was a legitimate cryptocurrency exchange and none of the warnings flagged any issues using the platform in the UK, or said there was a high scam risk.

And it is the nature of an IOSCO warning that matters, not just the presence of one. Mr K is right that we expect firms to take note of a warning within a month of it being posted, and to adapt their fraud measures accordingly (to whatever risk is highlighted by the content). Here I do not think that meant blocking all payments. The FCA issued a warning about 'K' that explicitly highlighted the risk of potential scams but this was not until 22 September 2023 so cannot be taken into account in this case.

This means what I need to decide is whether the bank's intervention at the time of payment 3 was proportionate. I am satisfied it was. It asked open questions and gave a relevant warning based on Mr K's answers. Unfortunately, as he was not honest the warning was not relevant to the risk he was exposed to. From the two calls the parties had, Halifax understood he was moving the money into his cryptocurrency account to hold for friends and

family and that he regularly invested in this way, he wasn't new to it. He said he hadn't been told not to discuss this with the bank and no one had told him to move the money. He was confident and forthright. He had been coached by the scammer not to disclose any details of the 'job opportunity' he was taking up. But there was nothing in his demeanour to give the bank an insight into the reality. As Mr K opted to give the bank incorrect information he prevented it from identifying the hallmarks of a job scam and warning Mr K accordingly.

I agree with the investigator that a further intervention at the time of payment 4 was warranted given the increase in payment value and destination, but I also agree that it would most likely have made no difference as Mr K would most likely not have disclosed the real payment purpose.

It follows I do not find Halifax can fairly be held liable for Mr K's losses.

I have then considered if Halifax did what we would expect to try to recover Mr K's losses when the scam was reported. As it was over a year after the scam and Mr K knew he had moved the money on from the recipient account to the scammer there was no realistic prospect of any recovery. So I find no failing on its part in this regard.

It follows I am not instructing Halifax to refund any money to Mr K. I do accept Mr K has fallen victim to a sophisticated scam and I am sorry he has had to experience this. I can understand why he would like to be compensated for his financial loss. But I don't consider that the bank, which had no involvement in the scam itself, can be fairly held liable for the reasons set out above.

My final decision

I am not upholding Mr K's complaint.

Under the rules of the Financial Ombudsman Service, I'm required to ask Mr K to accept or reject my decision before 8 September 2025.

Rebecca Connelley
Ombudsman