

The complaint

Mr K complains that Bank of Scotland plc trading as Halifax (Halifax) won't refund the money they lost as a result of a scam.

The complaint is brought on Mr K's behalf by a professional representative but for ease of reference I will refer to Mr K throughout the decision.

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.

Mr K has said he fell victim to three investment scams. He has advised that the investments were presented to him by someone he had been speaking to for several months ("the scammer") who he thought was his friend. Following her recommendation, he started to make several payments from his Halifax account towards what he thought were genuine investments.

Mr K has explained that he didn't do any research into the investments but that this was because he trusted the scammer. He has explained that he was added to group chats, attended regular video calls with other investors and had access to a platform in connection to the scams. He was also told to open cryptocurrency accounts with genuine providers which he used to send payments. Mr K has advised that the information shared by the scammer made the investments feel like genuine opportunities.

Mr K has told us he made a total of 20 payments towards the scam and lost a total of £24,678.96. From his sole account with Halifax he made 16 payments between May 2021 and July 2022. I have included a breakdown of the payments below:

Payment number	Date	Amount
1	21 May 2021	£5
2	21 May 2021	£740
3	21 May 2021	£35
4	24 May 2021	£100
5	6 January 2022	£100
6	17 January 2022	£220
7	11 February 2022	£10
8	11 February 2022	£10,200
9	11 February 2022	£200
10	9 May 2022	£203.96
11	16 May 2022	£95
12	15 July 2022	£100
13	18 July 2022	£100
14	18 July 2022	£4,500

15	25 July 2022	£2,900
16	25 July 2022	£1,700
	Total loss (not including any credits)	£21,208.96

Mr K realised he had been scammed by all three investments when he couldn't make any withdrawals. He also attempted an office visit for one of the scam firms and realised it didn't exist.

Mr K raised a complaint with Halifax. It investigated the complaint but didn't uphold it. It didn't think it had done anything wrong by allowing the payments to go through. So, Mr K brought his complaint to our service.

Our Investigator looked into the complaint but didn't uphold it. He thought the actions taken by Halifax were proportionate to the risk it identified.

Mr K didn't agree, so his complaint has been passed to me for review and a decision.

I issued my provisional decision on 20 October 2025. This is what I said.

I'm sorry to disappoint Mr K but I'm not upholding his complaint - for broadly the same reasons as the Investigator.

I'm aware that I've summarised this complaint briefly, in less detail than has been provided, and in my own words. No discourtesy is intended by this. Instead, I've focussed on what I think is the heart of the matter here. If there's something I have not mentioned, it isn't because I have ignored it. I haven't. I'm satisfied that I don't need to comment on every individual point or argument to be able to reach what I think is the right outcome. Our rules allow me to do this. This simply reflects the informal nature of our service as a free alternative to the courts.

The Lending Standards Board Contingent Reimbursement Model Code (CRM Code) provides refunds in certain circumstances when a scam takes place. But – it doesn't apply in this case. This is because it doesn't cover payments made to an account held in a person's own name. I've therefore considered whether Halifax should reimburse Mr K under any of its other obligations.

In broad terms, the starting position in law is that a bank is expected to process payments and withdrawals that a customer authorises it to make. It isn't disputed that Mr K authorised the payments from his Halifax account. Therefore, under the Payment Services Regulations 2017 and the terms of his account, Halifax is expected to process Mr K's payments, and he is presumed liable for the loss in the first instance.

But in some circumstances, it might be appropriate for Halifax to take a closer look at the circumstances of the payments – for example, if it ought to be alert to a fraud risk, because the transactions were unusual, or looked out of character or suspicious. And if so, it should have intervened, for example, by contacting the customer directly, before releasing the payments. This is to help protect customers from the possibility of financial harm from fraud. But I'd expect any intervention to be proportionate to the circumstances of the payment.

I've reviewed Mr K's account statements, and I can't conclude that Payments 1 to 7 would have looked particularly unusual or suspicious to Halifax. The highest payment made in relation to the scam up until this point was £740. These payments were relatively modest, so

I can't say Halifax should have been particularly concerned about them or that they would have presented an obvious scam risk in value alone.

Halifax have confirmed it intervened on Payment 8 when Mr K attempted to make a payment of £10,200. I think it was right to do this. This payment was for a significant amount and higher than all the other payments made by Mr K towards his cryptocurrency accounts. It provided Mr K with a written warning which I have included below:

"Just a minute.

Be sure that you know who you're sending money to.

Please check the account details with a trusted source. Fraudsters invent persuasive reasons to get you to make a payment.

See all the latest scams fraudsters use on our fraud hub page.

Failure to take precautions before you make your payment could mean we are not able to get your money back in the event of fraud.

What do you want to do."

Mr K expected Halifax to speak to him directly and ask questions about the payment before it was sent. But the payment was made in February 2022 to a cryptocurrency provider that Mr K had already sent several payments to across several months. And while there are known fraud risks associated with cryptocurrency, as scams like this have unfortunately become more prevalent, not all payments related to cryptocurrency are scam related.

There's also a balance to be struck between identifying and proportionately intervening in payments that could potentially be fraudulent, and minimising disruption to legitimate payments (allowing customers ready access to their funds). So, in the circumstances I think that a proportionate response was for Halifax to have provided a written warning about investment scams, drawing attention to the key features of this type of scam. In other words, while I would have expected it to intervene (as it did), I wouldn't have expected the intervention to go beyond an automated written warning.

Mr K has advised that better questioning at the time would have revealed the scam and prevented his losses. However, I'm not persuaded that a warning, even if it had gone into more detail, would have made a difference to Mr K's decision to go ahead with the payment or any later payments. I have provided my thoughts on this below.

- Mr K was convinced that he was dealing with genuine investments. He had been speaking to the scammer for several months before he began investing. He had formed a relationship with her and believed she was his friend. He also explained that he trusted her. He highlighted to our service that these investments were presented by people that he had known for over two years. He confirmed that he didn't do checks into the investments and relied on the information the scammer had shared before deciding to invest. This demonstrates the level of confidence he had in her judgement.*
- The information he has supplied us also shows that he was in regular contact with the scammer and that she was supplying him with information and helping him towards his investments. So, I can see why he thought he was dealing with genuine investments.*
- Mr K was added to group chats with other investors. He also attended regular online meetings with one scammer who shared updates with investors. He was impressed by the knowledge of the scammers. Mr K has also explained the scammers would hire large venues and host events. There were also thousands of investors, who were able to make withdrawals which made him think the investment was genuine.*

- *Mr K has explained he was required to complete a questionnaire, KYC documentation and was given access to trading accounts which made him think the investments were legitimate. He has also explained that he saw his profits increasing which he would monitor on a regular basis.*

It's clear that Mr K has been targeted and fallen victim to highly sophisticated scams. As explained above, he was convinced to invest by the scammer based on the relationship they had formed. It's also clear that he'd placed a significant level of trust in the scammer and was under her spell. The additional information around the group chats, regular meetings would have also added to the belief that he was dealing with legitimate businesses. So, on balance, I don't believe a warning would have impacted his decision to make the payments. I think it's more likely than not that Mr K would have disregarded any warnings as he wouldn't have thought it was relevant to his own circumstances. And on balance, I believe he would have continued to make the payments.

I also wouldn't have expected Halifax to intervene on any further payments as there wasn't a clear pattern of fraud. So, in the circumstances I don't think I can hold Halifax responsible for his losses.

Halifax offered Mr K £100 compensation for the delays in dealing with his complaint. I agree there has been some delays but overall, I think the offer made is fair in the circumstances of the complaint, so I won't be asking it to do anything further.

I have also considered whether Halifax could have done anything to recover Mr K's payments once the scam was uncovered, However, they were converted into cryptocurrency and paid to the scammers. Therefore, I don't think there was any realistic possibility of recovery.

I realise this means Mr K is out of pocket, and I'm really sorry he's lost money. However, for the reasons I've explained, I don't think I can reasonably tell Halifax to reimburse him.

Responses to my provisional decision

Halifax did not respond to my provisional decision.

Mr K didn't agree. In summary he said that Halifax has a duty of care to protect customers. He explained that Payment 8 should have triggered a more serious intervention. He also advised that the warning provided on this payment was generic.

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've reviewed Mr K's response to my provisional decision carefully, but the points he has made don't persuade me to reach a different conclusion.

Mr K believes that Payment 8 should have triggered a more serious intervention by Halifax and that the warning provided was generic. I have explained in my provisional decision why I didn't think a discussion was needed on the payment. Mr K had already sent a number of payments to the cryptocurrency provider across several months so in the circumstances I thought a proportionate response to Payment 8 was a written warning.

Mr K also believes the warning provided by Halifax was generic. But for the reasons explained in my provisional decision I don't think that better questioning at the time would

have revealed the scam and prevented his losses. Mr K had placed a significant level of trust in the scammer so I believe he would have continued to make the payments.

So, I don't think it would be reasonable to ask Halifax to refund the payments Mr K made.

My final decision

My final decision is that I'm not upholding the complaint.

Under the rules of the Financial Ombudsman Service, I'm required to ask Mr K to accept or reject my decision before 2 December 2025.

Aleya Khanom
Ombudsman