

## **The complaint**

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

The complaint is brought on Mr M's behalf by a professional representative. For ease of reading, I will refer to the actions and comments of the professional representative as being those of Mr M.

## **What happened**

The 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 M was introduced by his cousin to a cryptocurrency investment firm that I will call "C". Mr M has said he was added to a messaging group with C. He's told us this group included 1,000 other investors which made Mr M think this was a genuine investment. Mr M said he opened an account with C and was also advised to open a cryptocurrency account with a firm I will refer to as "P".

Mr M said he sent £4,001 between September and November 2023 as part of the scam. He received some returns from C on his initial investment. The payments were made by Open Banking to his account at P, and from there Mr M said he sent the money onto the scammers. He realised he had been scammed when he couldn't make a withdrawal and reported it to Halifax.

Mr M raised a complaint with Halifax in January 2024. Halifax 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 M brought his complaint to our service.

Our Investigator looked into the complaint but didn't uphold it. He didn't think the payments Mr M made were unusual and so he didn't feel Halifax should have identified a scam risk.

Mr M didn't agree. He said, in summary, that the payments were being made to a cryptocurrency exchange, and given the risks associated with cryptocurrency they should have been picked up and questioned by Halifax. He also explained that Halifax should have intervened when the payments were attempted, especially as they were made after the Consumer Duty had come into force, which he said puts obligations on businesses to prevent financial crime.

Mr M's complaint has now been passed to me for review and 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.

In line with the Payment Services Regulations 2017, consumers are generally liable for payments they authorise. Halifax is expected to process authorised payment instructions without undue delay. But Halifax also has obligations to help protect customers from financial harm from fraud and scams. Those obligations are however predicated on there having been a risk of loss to a fraud or scam present.

I think it's important to note here that although Mr M has provided some testimony about how he became involved in the scam, we've not been provided with any other evidence to show that he was caught up in this scam, such as evidence of his communications with the scammer. His representative has provided us with some generic information about the scam, but it doesn't link Mr M to the scam or demonstrate that he was a victim of it. And although he's shown us screenshots of his cryptocurrency statements showing withdrawals, they don't show that the withdrawals were related to the scam or that the funds were subsequently sent to the scammer. Generally, I would expect to see some more evidence to link the disputed payments to a scam, before considering if Halifax should have done anything else to intervene in the payments.

However, I don't think this makes a difference to the outcome of Mr M's complaint because, like the Investigator, I don't think Halifax ought reasonably to have identified the payments as suspicious or out of character, such that it ought to have intervened. So, I'm going to proceed on the basis that Mr M did suffer a loss to the scam he's described.

Halifax didn't identify that Mr M might be at risk of financial harm from a scam when he made the disputed payments. So, I need to decide if the transactions were concerning enough that I would have expected Halifax to have had a closer look at the circumstances surrounding them. But I also need to keep in mind that banks such as Halifax process high volumes of transactions each day, and that there is a balance to be found between allowing customers to be able to use their account and questioning transactions to confirm they are legitimate.

Mr M had held an account with Halifax for some time before he began to make payments to the scam – so Halifax did have some account history it could use to decide if the payments he made to the scam were suspicious or out of character.

I've reviewed Mr M's account statements, and I can't conclude that the payments made to the scam would have looked particularly unusual or out of character to Halifax. The highest payment made in relation to the scam was £500, but the majority of the disputed transactions were under £200. All the payments made 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. Mr M also made some higher value transactions in the months leading up to the scam, so the disputed payments were unlikely to have stood out as suspicious.

I've also considered the frequency of the scam payments and the fact they were being sent to a cryptocurrency exchange. The payments were made over a three-month period and although there was a slight escalation in frequency, I still wouldn't have expected that to have caused Halifax concern.

Mr M has advised that Halifax should have intervened as the payments related to cryptocurrency so it should have questioned them. The payments were made to a legitimate cryptocurrency exchange. 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. This means that I wouldn't expect Halifax to intervene on a payment just because it related to cryptocurrency. So, while Halifax should be looking out for signs that their customers are at risk of financial harm from fraud, I'm not persuaded the value or frequency of the payments were so unusual or suspicious for

Halifax to have suspected Mr M was at risk of financial harm - thereby prompting it to intervene before processing them.

I've also considered the comments Mr M has made regarding Halifax's obligations following the introduction of the Consumer Duty. However, given the information that was available to Halifax at the time Mr M made these transactions, I don't think the loss was foreseeable in these circumstances for the reasons I've explained above.

Taking all of this into consideration, I don't think Halifax ought to have done more before following the instructions Mr M gave.

I'm sorry to hear Mr M suffered a financial loss as a result of what happened. 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. For the above reasons, I think Halifax has acted fairly and so I'm not going to tell it to do anything further.

#### *Could Halifax have recovered Mr M's funds?*

There are industry standards around attempting recovery of funds where a scam is reported. So, I've also thought about whether Halifax could have done more to recover the funds after Mr M reported the fraud.

These payments were made through Open Banking, and they were converted into cryptocurrency and paid to a fraudster. Therefore, I don't think there was any realistic possibility of recovery.

I realise this means Mr M 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.

#### **My final decision**

For the reasons I've explained, I do not uphold this complaint against Bank of Scotland plc trading as Halifax.

Under the rules of the Financial Ombudsman Service, I'm required to ask Mr M to accept or reject my decision before 20 June 2025.

Aleya Khanom  
**Ombudsman**