DRN-5014854

The complaint

Mr F has complained that Bank of Scotland Plc (trading as "Halifax") failed to protect him from falling victim to a cryptocurrency investment scam and hasn't refunded the money he lost.

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

Mr F says that around February 2022 a colleague made him aware of an investment opportunity trading in cryptocurrency. He says he'd seen evidence of colleagues who'd invested and made returns so he decided to take part. Mr F later discovered that the alleged investment was fraudulent, and he says that as Halifax facilitated the payments without intervention, it's responsible for the losses that resulted.

Mr F added that the Financial Conduct Authority published a scam warning about the investment opportunity in March 2021, and he said that more recently a news outlet published an article outlining how the investment failed which left many investors out of pocket.

The payments Mr F made as part of the scam were as follows:

	Date	Amount
1	14/01/2022	£455
2	26/01/2022	£455
3	22/02/2022	£3,500
4	22/02/2022	£230
5	04/03/2022	£300
	Total	**£4,940**

In order to fund his supposed investment Mr F made the payments to his own wallet at a legitimate cryptocurrency platform. He then transferred the cryptocurrency from his wallet into cryptocurrency wallets directed by the scammer, believing that he was funding his own investment account. He realised he'd been scammed when he no longer had access to his investment account, nor the funds he believed it held.

Mr F made a complaint to Halifax. Halifax didn't uphold Mr F's complaint as it said the payments he made weren't out of character from his usual account activity, so it didn't have any concerns or reasons to intervene before they were made. It also noted that the payments were made to an account in Mr F's own name, that he had control of, before the

cryptocurrency was sent to the scammers. So it said it hadn't made any errors in allowing Mr F to make the payments.

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

Our investigator considered everything and didn't think the complaint should be upheld. He explained that he didn't think Halifax missed an opportunity to intervene and prevent the scam, because he didn't think Halifax ought to have considered the payments as suspicious.

As Mr F 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 F 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 F authorised these payments from leaving his account. It's accepted by all parties that Mr F 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 F'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.

I've seen Mr F's comments that he's entitled to a refund under the Contingent Reimbursement Model ("CRM") Code. But having considered this I'm satisfied that Halifax was correct to say that this scam isn't covered by the CRM Code. The CRM code covers scam payments made to third parties, but in this case, Mr F initially made the payments to his own account, that he had control of, at the cryptocurrency platform. As this isn't considered paying a third party, the payments aren't covered by the CRM Code.

I've carefully reviewed the transactions on Mr F's account in the months prior to the scam in order to build a picture of how he used his account. And having done so, I'm satisfied that it was fair for Halifax to allow Mr F to make the payments in questions without intervening.

Halifax should have recognised that payments to the cryptocurrency platform carried a level of risk, particularly given that the Financial Conduct Authority (FCA) and Action Fraud had been publishing warnings about scams involving cryptocurrency investments since mid-2018. So as these payments took place in late 2022, Halifax ought to have been aware of the potential risks associated with such transactions. But I wouldn't have expected Halifax to treat them as fraudulent purely because of that. Given the number of cryptocurrency transactions made every day, including the fact that many of them are legitimate, Halifax needed to consider a range of factors before deciding whether it should intervene before the payments were made.

Before deciding whether it needed to intervene to prevent potential financial harm, Halifax needed to assess the overall context of the payments, including the pattern in which they were made, the values involved, and Mr F's previous account activity. In this case, the

payments were not significantly out of character for Mr F, and the values weren't so high that they stood out as potentially fraudulent. Mr F regularly made transfers and debit card payments higher than the payments seen here, so I don't think Halifax ought to have been on notice that Mr F might've been falling victim to a scam.

Additionally, the pattern of payments – five transactions of fluctuating values spread over almost two months – isn't indicative of a scam, where payments are often made in rapid succession and tend to increase in size. Given this, it wasn't unreasonable for Halifax to process the payments without raising further queries or intervening in some other way beforehand.

I've noted Mr F's explanation as to how he was persuaded to invest by friends and colleagues whom he trusted – who were presumably also unaware they were part of the scam. I understand how Mr F would've been convinced by this and I fully accept he's the victim here. But it doesn't automatically follow that Halifax is responsible for his loss just because of that. Before asking Halifax to refund Mr F's losses I'd need to think that Halifax ought to have attempted to prevent the scam and that it failed to do so, but for the reasons I've explained, I don't think that's the case here.

Recovery of the funds

Mr F sent the funds to an account held in his own name, that he had control of, and he then used the funds to purchase cryptocurrency. Any of the funds he didn't use to purchase cryptocurrency would've remained within his control, and he'd have been able to use them as he chose. With this in mind, recovery wasn't an option for Halifax, so it's not something I'd have expected it to pursue.

I'm very sorry that Mr F 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 F's 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 26 March 2025.

Sam Wade
Ombudsman