DRN-5214258

The complaint

Mr K is unhappy that Bank of Scotland plc trading as Halifax didn't refund him after he told it he had fallen victim to a scam.

Mr K is represented in this matter by a claims management company, but for ease of reading I'll only refer to Mr K in this decision.

What happened

The background to this complaint is well known to both parties so I don't intend to set it out in full here.

In summary, between June and December 2023, Mr K transferred a total of £39,875 to a crypto wallet he held.

Mr K has told this service that he was introduced to the scammer by a close family member in June 2023. He understood that the scammer was a representative of a bank. The scammer offered Mr K an 'investment opportunity' and said he would trade on Mr K's behalf, promising substantial returns.

From June 2023 to December 2023, Mr K says he sent £39,875 to the scam platform via his cryptocurrency wallet. Mr K says he then became aware of 'irregularities' with the FCA registration for the business the scammer claimed to be working for. He says he raised his concerns with the scammer and was advised to move to a different investment platform. I understand that Mr K then tried to withdraw his funds. When he couldn't do so, he realised he had fallen victim to an investment scam.

Date	Transfer to	Amount
9 June 2023	Crypto wallet	£10
15 June 2023	Crypto wallet	£5,000
15 June 2023	Crypto wallet	£3,850
13 July 2023	Crypto wallet	£4,450
8 September 2023	Crypto wallet	£4,335
13 November 2023	Crypto wallet	£4,500
16 November 2023	Crypto wallet	£4,000
17 November 2023	Crypto wallet	£500
18 November 2023	Crypto wallet	£2,000
20 November 2023	Crypto wallet	£2,000
18 December 2023	Crypto wallet	£9,500
	Total transferred:	**£39,875**

Mr K complained to Halifax. He said it had failed in its duty of care to protect him from the scam.

Halifax didn't uphold Mr K's complaint. It noted that the payments Mr K had made had been between his own accounts. It explained that the Contingent Reimbursement Model doesn't cover transactions between a customer's own accounts. It said it had twice blocked the payments and only allowed them to proceed after it had spoken to Mr K and taken steps to establish that Mr K was aware of the risks associated with investing in cryptocurrencies and was not being pressured or encouraged by a third party to make the transfers.

It also said it hadn't felt there was any reason for it to intervene any sooner than it did as the disputed payments were not out-of-line with Mr K's usual account activity, including making multiple payments on the same day.

Our investigator said she didn't think Mr K's complaint should be upheld. She noted that Halifax had blocked the payment Mr K attempted to make on 13 July 2023, and only allowed it to proceed after Mr K had discussed the transaction with its fraud team. It had also blocked the payment Mr K made on 18 December 2023 and did not allow the payment to proceed until Mr K had again spoken to its fraud team.

She said she was of the view that even if Halifax had intervened sooner, when Mr K attempted to make the second transfer on 15 June 2023, she felt that it would not have led Mr K to act any differently. She said she had reached this view as when Halifax did discuss the fourth payment (13 July 2023) and the eleventh payment (18 December 2023) Mr K confirmed he still wanted to go ahead with these payments despite warnings and questioning from Halifax. She noted that on both occasions Halifax warned Mr K of the high-risk nature of cryptocurrency related transactions and in both interventions, Halifax asked Mr K if any third party was involved in the decision making, such as an account manager, coach, or trader. Mr K said no third party was involved.

Mr K's representative did not accept our investigator's view. In summary, it said it did not think the interventions Halifax had made were sufficiently 'robust'. It said Halifax should have asked for extensive details about the investments and should also have asked for information about Mr K's personal circumstances and any vulnerabilities he had.

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 hear that Mr K has lost money in a cruel scam. It is not in question that he authorised and consented to the payments in this case. So, although Mr K didn't intend for the money to go to a scammer, he is presumed to be liable for the loss in the first instance. This is because, in broad terms, the starting point 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 and the terms and conditions of the customer's account. I have taken this into account when deciding what is fair and reasonable in this case.

I must also take into account the law, regulatory rules and guidance, relevant codes of practice and what I consider to have been good industry practice at the time. I think Halifax should fairly and reasonably:

- have been monitoring accounts and any payments made or received to counter various risks, including anti-money laundering, countering the financing of terrorism and preventing frauds 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 frauds 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.

I need to decide whether Halifax acted fairly and reasonably in its dealings with Mr K when he made the payments, and whether it should have done more than it did.

The Lending Standards Board Contingent Reimbursement Model (CRM code) provides for refunds in certain circumstances when a scam takes place. However, it does not apply in this case. This is because it does not apply to payments made to an account held in the customer's name; Mr K has confirmed that the crypto wallet was held in his name.

I have also considered whether the payments Mr K made were out-of-line with his usual use of his account. Having done so, I don't think the payments were out-of-line with his normal pattern of account usage. In particular, I note Mr K had previously transferred similar and higher amounts to those lost in the scam, for example £4,000 on 15 December 2022, £5,150 on 22 December 2022, £2,000 on 6 January 2023, £6,000 on 6 February 2023, £2,500 on 22 February 2023, £3,200 on 22 May 2023 and £5,000 on 24 May 2023. I also note that Mr K had previously sent multiple payments on the same day. In view of this I don't think that Halifax would necessarily have had cause for concern when Mr K made two payments to his crypto wallet on 15 June 2023.

I have also listened to the conversations Mr K had with Halifax when it blocked the payments on 13 July 2023 and 18 December 2023. I note that Mr K's representative has said that it does not feel these interventions were sufficiently robust and that Halifax should have asked for extensive details about the investments Mr K intended to make and his personal circumstances.

I am mindful that in both the calls Halifax explained to Mr K that he was speaking to its fraud team and that the transaction he was trying to make had been flagged up as a '*higher than normal risk of a scam'*. In both calls Mr K told Halifax that there was no third party involvement and that he was acting on his own behalf. I note that Halifax queried this to confirm that no broker, coach or investment adviser was involved in the transactions Mr K was making. On both occasions Mr K confirmed that there was no third party involvement.

In the second intervention in December 2023, Mr K told Halifax that he transferred funds from his crypto wallet to a trading account he also held in his own name. He confirmed that no one else was involved in the trades he was placing and said, '*I just do it myself*.' He also said he had transferred profits from this trading account back to his crypto wallet, in particular he referred to a withdrawal of around £9,500 in November 2023 he had made from his trading account. I am also mindful that in the second call in December 2023, when asked if he had been contacted by any third party about the transfers or investments he said, *'The only person I've been contacted by is Halifax.'*

As Mr K told Halifax on both occasions that there was no third party involvement and that the crypto wallet and the investment account were both held in his name and under his control - and that he understood the risk warnings Halifax discussed with him - I don't think there was more that Halifax could reasonably have been expected to do.

I note that Mr K's representative says Halifax should have asked Mr K to attend a branch for a face-to-face meeting to discuss the blocked payments. I have considered this point. Having done so, as Mr K had on two separate occasions confirmed to Halifax that there was no third party involvement, that he was making his own investment decisions and no one had access to his accounts I can't reasonably say that Halifax should have refused to unblock the payments until Mr K had attended a branch interview.

I do understand that this is not the decision Mr K was hoping for, but I am satisfied that Halifax acted reasonably in alerting Mr K to the risks he was taking and he confirmed at both interventions that he wanted to go ahead. Having carefully considered this matter my decision is that Halifax does not need to refund any of the money Mr K has lost in this scam.

My final decision

My decision is that, for the reasons I have set out above, I do not uphold this complaint.

Under the rules of the Financial Ombudsman Service, I'm required to ask Mr K to accept or reject my decision before 13 February 2025.

Suzannah Stuart
Ombudsman