DRN-6055374

The complaint

Mr R complains that Bank of Scotland Plc trading as Halifax won't refund him the money he lost in an investment scam.

Mr R is being represented by a professional representative.

What happened

The circumstances surrounding this complaint are well known to both parties, so I won't repeat them in detail here. Instead, I've summarised what I consider to be the key points.

Mr R received an unsolicited message on a popular messaging application, on 15 January 2021. He struck up a conversation over the messaging application, which turned to cryptocurrency investment after a short while. Mr R was already investing elsewhere but he was persuaded to invest through the same investment platform as his new friend. He was promised a full return of his capital with profits of over 200% over six months, with no risk and no withdrawal fees. He did some research, mainly through links sent to him by his new friend and he set up an account with a cryptocurrency provider, which he was to use to transfer funds to his new investment.

He made a series of payments from his Halifax account to his cryptocurrency account over the next four months, which were used to fund payments to his investment account. Unfortunately, when Mr R tried to withdraw some of his investment, he was told he needed to pay the equivalent of 25% of the value of his investment as a withdrawal fee before he would be able to access his investment and withdraw it. At this point, he realised he had been the victim of a scam.

Mr R made the following payments (and received the following returns) as part of this scam:

Payment	Date	Amount	Payment type	Destination
1	20/01/2021	£1,870	Faster payment	Own cryptocurrency account
2	23/01/2021	£200	Card payment	Own cryptocurrency account
3	25/01/2021	£75	Card payment	Own cryptocurrency account
4	25/01/2021	£10	Card payment	Own cryptocurrency account
5	25/01/2021	£70	Card payment	Own cryptocurrency account
6	08/02/2021	£10	Card payment	Own cryptocurrency account
7	10/02/2021	£500	Card payment	Own cryptocurrency account
8	10/02/2021	£300	Card payment	Own cryptocurrency account
	24/02/2021	*£701.72*		*Credit*
9	16/03/2021	£38	Card payment	Own cryptocurrency account
	18/03/2021	£44.37		*Credit*
	23/03/2021	*£714.64*		*Credit*
	07/04/2021	*£711.89*		*Credit*
10	14/04/2021	£1	Faster payment	Own cryptocurrency account
11	15/04/2021	£7,300	Faster payment	Own cryptocurrency account
12	15/04/2021	£486	Faster payment	Own cryptocurrency account
	15/04/2021	*£70.34*		*Credit*

13	23/04/2021	£3,500	Faster payment	Own cryptocurrency account
14	25/04/2021	£125	Faster payment	Own cryptocurrency account
	26/04/2021	*£193.55*		*Credit*
15	06/05/2021	£1,800	Faster payment	Own cryptocurrency account
16	06/05/2021	£200	Faster payment	Own cryptocurrency account
	06/05/2021	*£50*		*Credit*
17	11/05/2021	£3,500	Faster payment	Own cryptocurrency account
18	11/05/2021	£150	Faster payment	Own cryptocurrency account

Mr R says Halifax should have intervened and asked probing questions about the payments, providing him with clear and relevant warnings. The payments were out of character for the account and some of the payments were large. If Halifax had questioned the payments and provided appropriate warnings, he wouldn't have made these payments. He also says he was vulnerable at the time he made the payments.

Halifax says all the payments were transfers to another account belonging to Mr R, so the Contingent Reimbursement Model (CRM) Code doesn't apply. The payments didn't trigger any fraud alerts. It didn't have any reasonable prospect of recovering Mr R's money once he reported the scam. In particular, it said it had no chargeback rights for card payments that successfully credited a legitimate account belonging to Mr R. Halifax didn't think Mr R had a reasonable basis for believing that this investment was genuine, as he had been contacted unexpectedly over social media, was promised high returns that ought to have raised doubts that the investment was legitimate and he carried out limited research before investing.

The Investigator didn't uphold Mr R's complaint. He didn't think any of the payments were sufficiently unusual to have warranted intervention from Halifax. In any event, if Halifax had intervened, he considered a general written warning about scam risks would have been proportionate, given all the circumstances. He didn't think such a warning would have led Mr R to stop making payments. He said the evidence showed Mr R followed the advice of the scammer. There was evidence in the copies of the messages sent between Mr R and the scammer that he had been told by someone that the investment was a Ponzi scheme, but it didn't lead him to stop investing. He also considered Mr R was very confident in the investment, to the point that he had persuaded friends and family to invest. He said Halifax didn't have any reasonable prospect of recovering Mr R's money because it had been sent on to his own account with a cryptocurrency exchange and then promptly transferred on from there.

Mr R didn't accept the Investigator's conclusions. He thought the payments were highly unusual for his account, in terms of the size of payments and the frequency with which they were made. Money was paid into the account and quickly paid out again, to a cryptocurrency account, and the payments were generally escalating in value. He thought this combination of risk factors meant Halifax should have intervened more directly. He asked for his complaint to be passed to an ombudsman for 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.

Having done so, I'm not upholding Mr R's complaint. While I understand this will come as a disappointment to Mr R and I am conscious of the impact this cruel and distressing scam has had on him, I'm not persuaded that I can fairly conclude that Halifax is responsible for his losses. I say this because I don't consider further intervention would have uncovered the scam. I'll explain why.

In broad terms, the starting position is that a bank is expected to process payments and withdrawals that a customer authorises it to make, in accordance with the accounts terms and conditions and with the Payment Services Regulations (PSRs). It isn't in dispute that Mr R authorised these payments. Halifax had an obligation to process the payments, but that isn't the end of the story.

The Contingent Reimbursement Model (CRM) Code doesn't apply here. This code doesn't apply where payments are made between two accounts controlled by the same customer, or where payments were made by debit card. Since all of the payments were to Mr R's cryptocurrency account and some of the payments were also made by debit card, they don't fall within the scope of the CRM code.

But, I've also taken into account the regulator's rules and guidance; relevant codes of practice, along with what I consider to have been good industry practice at the time. Having done so, I consider Halifax should have fairly and reasonably been on the lookout for the possibility of Authorised Push Payments scams (amongst other things) at the time, and intervened if there were clear indications its customer might be at risk.

Halifax does have a difficult balance to strike in how it configures its systems to detect unusual activity that might indicate its customers are a higher risk of fraud. It would not be reasonable or possible for Halifax to intervene in every transaction it processes. I would expect intervention to be proportionate to the circumstances of the transaction.

In Mr R's case, I wouldn't have expected Halifax to intervene on payments 1-10, given that they were relatively small payments, they didn't follow a particular known pattern of fraud and the frequency and size of payments was very irregular, with some very low value payments, sometimes being made a few times in the same day, and then over a month separating other payments. While the first payment on 20 January 2021 was higher in value than the transactions Mr R usually made on his account, he did occasionally make higher value payments from his account, so I don't think that payment would have appeared particularly suspicious.

My conclusions differ slightly from the Investigator, because I consider Halifax ought to have intervened on payment 11. The value of this payment was significantly higher than the usual payments Mr R made from his account. Mr R rarely made payments of more than a few hundred pounds and the account generally had a low balance, typically under £250 and often much less. There is only one instance of Mr R making a payment for over £1,000 in the months leading up to this series of transactions and payment 11 was more than three and a half times greater than the next largest transaction Mr R had made, going by the account statements Halifax has provided.

While Mr R points to other risk factors that he says should have led to strong intervention from Halifax, I think the size of the payment was the main reason why Halifax should have intervened. It was quite common for Mr R to make repeated payments to the same payee, sometimes several times on the same day. This payee had become reasonably well established by the time of payment 11, having been set up around three months earlier and with several payments having been sent to, and received from that account. The payments he had received back from that account amounted to over £2,000, so they were reasonably substantial too.

The general pattern of these payments was one of relatively low value, irregular amounts being sent to a cryptocurrency exchange over a period of several months, with occasional larger payments. While the larger payments were often funded with a large deposit into the account shortly beforehand, that's consistent with how Mr R used the account for other, slightly larger transactions, with the account generally being maintained with a low credit

balance, and where larger payments were made they were made with amounts being deposited into the account and then paid out promptly.

I've taken into account that these payments were made to a cryptocurrency exchange. At the time these payments were made, I think it was reasonable for Halifax to take into account a range of factors when deciding whether to make further enquiries of its customer about a particular payment. In this case, the pattern of payments wasn't necessarily consistent with fraud – irregular, relatively low value payments, not always increasing in value – and did not, in my view, indicate a heightened risk of financial harm. I don't think there were sufficient risk factors in place for payment 11 to have meant Halifax ought to have intervened in person and spoken with Mr R directly, as he has suggested they should have done. However, I do consider a written warning outlining the general scam risks would have been appropriate.

I agree with the Investigator's overall conclusion, that a written warning is unlikely to have led Mr R to stop making payments. Such a warning would have been general in nature, for example it might have warned about situations where a customer was told their account was at risk and they were being asked to move money to another account urgently, amongst other things. I don't think such a warning would have resonated with Mr R and the particular circumstances he was facing.

Even if a tailored warning had been provided, relevant to cryptocurrency investment scams, it is not clear to me that it would have been effective either. Such a warning might have cautioned Mr R to beware of unrealistic investment returns, to check that he could make withdrawals, or to carry out research, for example. Factors such as the reasonably substantial monthly returns Mr R had received back from his investment are likely to have given him greater confidence that the investment was legitimate and made it less likely he would have responded positively to a scam warning from Halifax. I also note, from the copies of the messages Mr R exchanged with the scammer, that Mr R seems to have been told this might be a scam, albeit relatively late on. He mentions being told about this investment being a scam around 7 May 2021, but he doesn't seem to have carried out further research or sought guidance, except by querying it with the scammer. He seems to have been reassured and went on to make further payments.

Overall, despite my natural sympathy for Mr R, while I do consider Halifax could and should have done more here, on balance I'm not persuaded that the evidence shows that proportionate intervention is likely to have led to Mr R's losses being prevented, for the reasons given above.

In terms of recovering Mr R's money, I agree with the Investigator that there wasn't any reasonable prospect of Halifax being able to recover his money. The card payments were successfully completed, with money being credited to Mr R's account with his cryptocurrency exchange. In those circumstances, it wouldn't have been possible to raise successful chargeback claims under the card scheme rules. And the money Mr R sent to his cryptocurrency account was promptly paid out to the scammers, so there wouldn't have been any money in Mr R's cryptocurrency account for Halifax to attempt to recall even if it had tried to raise a claim with the cryptocurrency exchange.

My final decision

I don't uphold Mr R's complaint.

Under the rules of the Financial Ombudsman Service, I'm required to ask Mr R to accept or reject my decision before 9 March 2026.

Greg Barham
Ombudsman