DRN-5385887

The complaint

Mr R is unhappy that Bank of Scotland plc, trading as Halifax, will not refund the money he lost as the result of an investment scam.

Mr R has used a representative to bring his complaint to this service. For ease, I will refer solely to Mr R throughout this decision.

What happened

As both parties are familiar with the details of the scam I will not repeat them here in full. In summary, Mr R fell victim to a cryptocurrency investment scam. He made the following payments to his existing Binance account by debit card, and from there he transferred the crypto onto the scammer believing he was then investing through firm 'B'.

payment	statement date	value
1	18.03.2024	£100
2	03.04.2024	£1,070
3	08.04.2024	£1,999.35
4	09.04.2024	£2,000
5	09.04.2024	£2,000
6	15.04.2024	£1,800
7	17.04.2024	£2,600
8	18.04.2024	£1,776.88
9	23.04.2024	£183.39
10	23.04.2024	£2,496.26
11	29.04.2024	£1,000
12	30.04.2024	£680.50
13	03.05.2024	£1,845.73
14	03.05.2024	£2,500

Mr R realised it was a scam after his trading account was frozen and he was told to pay certain fees before he could access his funds. He reported this to Halifax on 8 May 2024.

Mr R says Halifax did not do enough to protect his money. Halifax says Mr R did not carry out adequate checks before investing. It says it asked Mr R to verify all payments except 1, 5 and 9 through its banking app. It explained it could not raise chargeback claims as the payments were to an account in Mr R's own name.

Our investigator upheld Mr R's complaint in part. She said Halifax ought to have contacted Mr R before processing payment 5 and had it done so it would most likely have stopped the scam. But as Mr R could have done more to check the investment opportunity, he should share liability for the losses from payment 5 onwards.

Mr R accepted this assessment. Halifax did not and asked for an ombudsman's review. It

said the transactions were not out of character for Mr R's account. He had sent money to his Binance account across a number of transactions with similar frequency in January 2024. It added it was not the point of loss in the scam and Mr R's own checks before he made the payments were inadequate.

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 don't dispute Mr R was scammed and he wasn't making payments for the reason he thought he was, but I remain satisfied the transactions were authorised under the Payment Services Regulations 2017.

It's also accepted that Halifax has an obligation to follow Mr R's instructions. So in the first instance Mr R is presumed liable for his loss. But there are other factors that must be considered.

To reach my decision I have taken into account the law, regulator's rules and guidance, relevant codes of practice and what was good industry practice at the time. To note, as the payments were made by debit card and to an account in Mr R's own name the principles of the Contingent Reimbursement Model (CRM) code do not apply in this case.

This means I think that Halifax should have:

- been monitoring accounts and payments made or received to counter various risks, including fraud and scams, money laundering, and the financing of terrorism.
- had systems in place to look out for unusual transactions or other signs that might indicate that its customers were at risk of fraud (amongst other things). This is particularly so given the increase in sophisticated fraud and scams in recent years, which financial institutions are generally more familiar with than the average customer.
- acted to avoid causing foreseeable harm to customers, for example by maintaining adequate systems to detect and prevent scams and by ensuring all aspects of its products, including the contractual terms, enabled it to do so;
- in some circumstances, irrespective of the payment channel used, taken additional steps or made additional checks before processing a payment, or in some cases declined to make a payment altogether, to help protect its customers from the possibility of financial harm.
- been mindful of – among other things – common scam scenarios, how the fraudulent practices are evolving (including for example the common use of multi-stage fraud by scammers, including the use of payments to cryptocurrency accounts as a step to defraud consumers) and the different risks these can present to consumers, when deciding whether to intervene.

In this context I think Halifax should be liable in part for payments 5 to 14. I'll explain why.

Payments 1 to 4

There is a balance to be struck. Banks and building societies have obligations to be alert to fraud and scams and to act in their customers' best interests. But they can't reasonably be involved in every transaction. I don't think it was unreasonable for Halifax to process these payments without further checks given their values and the stage in the scam.

Payment 5 onwards

I think Halifax ought to have contacted Mr R before processing this transaction. It established a pattern typical of scams as the fourth payment in less than a week to an identifiable cryptocurrency platform. There was a trend of increasing value and it took the total spend in two days to this beneficiary account to £5,999.35. And the payments were funded by a preceding credit onto the account.

Halifax argues the payments were not out of character for the account, relying on Mr R's pattern of payment to the same recipient account in January 2024. But I disagree. The payments in January were much lower value, bar one, and after that outlying higher payment the average transaction values fell sharply.

Halifax also says it was not the point of loss in the scam. I appreciate that Mr B's loss didn't materialise directly from his Halifax account, but even though he was transferring funds to a crypto account in his own name, I still think that Halifax ought to have taken a closer look at payment 5 given the elevated risk of fraud associated with cryptocurrency investments which was well established by this time. Given the warnings from the FCA and Action Fraud started years before in mid-2018 it is reasonable to say by April 2024 Halifax ought to have had a good understanding of how crypto scams works – including the fact that their customer often moves money to an account in their own name before moving it on again to the fraudster.

Therefore, I'm satisfied that Halifax should've had mechanisms in place to detect and prevent this type of fraud at the time Mr R was making this payment, and that it should have led to it intervening to ask further questions about payment 5.

This means I now need to decide what would most likely have happened had Halifax spoken to Mr R at this stage. I would expect Halifax to have asked Mr R what the payment was for, and for the basic surrounding context of the payment - it could, for example, have asked how he had been contacted, whether the contact was expected or unsolicited, whether he'd parted with personal details in order to open a trading account, whether he was being helped by any third parties, what returns he was expecting, what research had he conducted and had he sought any independent advice? I believe such questions asked in an open and proportionate manner would have shown many of the typical features of cryptocurrency scams in this case. Mr R had been contacted unexpectedly via a messaging platform with a mixed reputation, he had little experience and hadn't taken any independent advice to verify the opportunity, and he'd been promised unrealistic returns of between 30 and 60%.

I have no reason to believe Mr R wouldn't have been open with Halifax, and I think he would have taken its intervention seriously. So I think Halifax would have quickly learned from its conversation with Mr R the basic background to the payment instruction – that he was buying cryptocurrency through Binance to send onto what he thought was a cryptocurrency trading investment which he'd decided to pursue after learning about it via a messaging app. From the available evidence I cannot see that Mr R had been provided with a cover story by the scammer in the event he was asked by the bank about the reason for the transfer(s).

Even though the conversation would have identified the payment was going to Mr R's own cryptocurrency account (before being sent onto the scammers), the conversation shouldn't have stopped there on the basis that the money appeared to be going to somewhere safe and within Mr R's control. As I have said, by 2024 Halifax was well aware – or ought to have been well aware – of how scams like this work – including that the customer often moves money onto an account in their own name before moving it on again to scammers.

So, in the round, I think Halifax would have been concerned by what the conversation would most likely have revealed and so warned Mr R, explaining the typical characteristics

of scams like this. Had it done so I think Mr R would have listened, recognised he was at risk and had second thoughts.

It follows I think Mr R would not have gone ahead with payment 5, nor any subsequent payments so it is reasonable to hold Halifax liable for the losses from payment 5 onwards.

I've then considered carefully whether Mr R should hold some responsibility for his loss by way of contributory negligence. Accepting that he is not the fraud expert - that is the role of Halifax, I do think he missed some clear signs that the opportunity might not be legitimate. I say this as he went ahead based on an unsolicited contact on a messaging app. This is not the typical approach from investment professionals. The returns he was promised were high which ought to have triggered more questions. From his testimony it seems he did very little independent research. He has said just that he found no negative reviews and the site the scammer directed him to looked very professional. Overall, Mr R was willing to invest significant sums without an appropriate level of due diligence when, by his own admission, he had very little prior investment experience. And so I find it is fair that he shares the liability for his loss equally with the bank.

Did Halifax do what it should to try to recover Mr R's money?

As he made all the payments using his debit card, the only potential recovery option would have been through the chargeback scheme.

The chargeback process is voluntary and run by the card scheme whereby it will ultimately arbitrate on a dispute between the merchant and customer if it cannot be resolved between them after two 'presentments'. Such arbitration is subject to the rules of the scheme — so there are limited grounds on which a chargeback can succeed or be deemed a 'valid claim'.

Our role in such cases is not to second-guess the card scheme rules, but to determine whether the regulated card issuer, so here Halifax, acted fairly and reasonably when presenting (or choosing not to present) a chargeback on behalf of its customer.

I can see that Halifax did not attempt any chargeback claims. When the payments were made to Mr R's Binance account and exchanged for cryptocurrency, the 'service' he paid for was provided. So he had no grounds for dispute with the exchange. Also that under the card scheme rules there are no chargeback rights for any subsequent purchase for goods or services from a digital wallet. Overall, I have found no grounds to challenge the bank's decision not to raise any chargeback claims for the payments.

Putting things right

- Refund 50% of payments 5 to 14.
- Pay 8% simple interest on this amount, to be calculated from the date of payment until the date the settlement is made.*

*If Halifax deducts tax from the interest element of this award, it should provide Mr R with the appropriate tax certificate so he can submit a claim to HMRC if applicable.

I have found no grounds to award any additional compensation in the circumstances of this case.

My final decision

I am upholding Mr R's complaint in part. Bank of Scotland plc, trading as Halifax, must put things right as set out above.

Under the rules of the Financial Ombudsman Service, I'm required to ask Mr R to accept or reject my decision before 6 June 2025.

Rebecca Connelley
Ombudsman