

The complaint

Mrs R complains that Bank of Scotland plc trading as Halifax (“Halifax”) won’t refund her the money she lost, after she fell victim to an Authorised Push Payment (“APP”) investment scam.

What happened

The background to this complaint is well known to both parties, so I won’t repeat it in detail here. But in summary I understand it to be as follows.

In or around August 2022, Mrs R was actively looking for investment opportunities. Following research she carried out online, Mrs R made an enquiry to what she thought was a genuine company. She was subsequently contacted by the company and discussed investment plans with them. Mrs R has said she carried out further research online and saw positive reviews about the company. Believing everything to be genuine, Mrs R decided to invest and was instructed to set up an account with a legitimate cryptocurrency exchange platform.

Mrs R started with modest investments, making payments into a cryptocurrency wallet in her name, before moving the funds on to what she was told was the investment company’s trading platform. She could see profits being made at a reasonable rate and was able to make some withdrawals from her account; the first withdrawal being made with the support of an ‘account manager’ that had been assigned to her.

It was suggested to Mrs R that she make further investments, to enable her account to be upgraded from basic to advanced. Confident with what she’d seen, Mrs R decided to make further payments. But unknown to her at the time, Mrs R was dealing with fraudsters and the payments she was making from her wallet were going to accounts the fraudsters controlled. Mrs R realised she’d been scammed when contact with the investment company started to fade and when she was asked to make a final payment in order to keep her account running.

Between 2 September 2022 and 3 November 2022, Mrs R made 5 payments from her Halifax account to her cryptocurrency wallet and then on to the fraudsters, totalling £24,850. During this time she made two withdrawals totalling £997.67. A breakdown of these transactions is listed below;

2/9/2022	payment to cryptocurrency wallet	£20
7/9/2022	payment to cryptocurrency wallet	£30
7/9/2022	withdrawal from cryptocurrency wallet	£85.51
7/9/2022	payment to cryptocurrency wallet	£3,500
27/9/2022	payment to cryptocurrency wallet	£20,000
3/11/2022	withdrawal from cryptocurrency wallet	£912.16

Mrs R raised the matter with Halifax. It looked into Mrs R’s complaint and issued its final response in March 2023 not upholding it. In summary this was because it thought the activity on Mrs R’s account was in line with her previous account activity, so it said it had no reason to intervene.

Unhappy with Halifax's response, Mrs R brought her complaint to this service. One of our Investigator's looked into things but didn't think the complaint should be upheld. In summary he didn't think the payments would have appeared as particularly unusual or suspicious in appearance, when considering Mrs R's normal account activity. So he didn't think the payments should have flagged to Halifax for these reasons. He added that because the payments were made to a cryptocurrency wallet, then moved to the scammer, any recovery would have been unsuccessful.

Mrs R didn't agree with our Investigator's view. As agreement couldn't be reached the complaint has been passed to me 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.

There is no dispute that the transactions were 'authorised payments', even though Mrs R was the victim of a sophisticated scam. Mrs R made the payments herself and under the relevant regulations, and the terms and conditions of her account, Mrs R is presumed liable for the loss in the first instance.

However, taking 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 consider 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 fraud and scams;
- Have had systems in place to look out for unusual transactions or other signs that might indicate 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 banks are generally more familiar with than the average customer; and
- 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.

So, I consider that as a matter of good practice, Halifax should have been on the lookout for unusual and out of character transactions.

In the circumstances of this case, I think it is finely balanced as to whether the activity that took place on Mrs R's account during the scam was sufficiently unusual and out of character to give Halifax cause for concern that she was at risk of fraud. Having reviewed the first disputed transactions made between 2 and 7 September 2022, I don't think these were enough in themselves to have warranted an intervention by Halifax, as they were not so unusual as to amount to a significant deviation in the way the account was normally run.

However, by the time Mrs R made the payment for £20,000 on 27 September 2022, it's arguable that this marked a significant increase in spending, to the point where Halifax could potentially have intervened and questioned Mrs R before allowing the payment to be processed. On the one hand the payment was large in value. But on the other hand, looking at Mrs R's account history, there have been large transactions on her account previously.

I'm also mindful that at the point this payment was made, the payments were being made to an existing payee - a cryptocurrency account Mrs G held to which, by this point, she had made and received a number of other payments. And whilst cryptocurrency can be utilised by scammers, I would not expect Halifax to be on notice about every payment that goes to the platform Mrs G was using, as many people use it for legitimate purposes.

But in any event, in the individual circumstances of this case, even if I considered Halifax should have intervened further than it did, I don't think it would have made a difference. I'll explain why.

In such circumstances, whilst Halifax had no duty to protect Mrs R from a bad bargain, or give investment advice, it could have asked some further questions to ascertain whether Mrs R was likely to be at risk of financial harm from fraud. I've thought carefully about the sorts of questions Halifax could've asked, bearing in mind the features of investment scams at that time.

However, even if Halifax had intervened at this point and asked further questions about the nature of the payment Mrs R was making, I'm not persuaded it would have likely stopped her from proceeding or have ultimately prevented her loss. I say this for a few reasons. First, Mrs R had been able to make withdrawals, which reassured her. So, if Halifax had warned her about not being able to withdraw her money, I don't think it would have led her to believe she was being scammed.

Alongside this, Mrs R wasn't cold called or promised returns that were too good to be true, both of which are common features of this type of scam. Rather, here Mrs R had proactively been looking to invest and was contacted after making an enquiry. And while she could see what she thought at the time to be profits being made on her account, she's said the profits seemed reasonable and not too drastic when considering the amount being invested. Mrs R has also explained that she'd carried out her own research and found positive reviews and a professional looking website. And has said she had no reason to believe this was a scam.

So, even if Halifax had intervened and provided Mrs R with a scam warning, I'm not persuaded it would have dissuaded Mrs R from continuing with her payments. I think it more likely than not that the answers Mrs R would have given, to any questions Halifax could reasonably have been expected to ask, wouldn't have concerned it that Mrs R was about to fall victim to an investment scam. There were no obvious indicators of what I consider to be well published investment scam typologies at the time.

I think as a result it's more likely than not Halifax would've been satisfied Mrs R wasn't at risk of falling victim to an investment scam and that Mrs R would've felt comfortable continuing with the payments.

So overall, for the reasons I've explained, I don't think Halifax's failure to intervene can reasonably be considered as the proximate cause of Mrs R's loss in these circumstances, as it seems likely she would have proceeded to make the transactions irrespective of any intervention by the bank.

I've also considered what attempts Halifax made to recover the funds from the fraudsters. Unfortunately, as the payments went to a cryptocurrency account in Mrs R's name, before being sent on to accounts the fraudsters controlled, Halifax would not have had the opportunity to successfully recover any of the money Mrs R lost.

I want to stress that I feel considerable sympathy for what Mrs R has been through here. She has lost a significant amount of money to what was a cruel and sophisticated scam. But

unfortunately, whilst I'm sorry to have to disappoint her, I'm not persuaded that this was a consequence of any specific failing on the part of Halifax.

My final decision

My final decision is that I don't uphold this complaint.

Under the rules of the Financial Ombudsman Service, I'm required to ask Mrs R to accept or reject my decision before 26 February 2024.

Stephen Wise
Ombudsman