DRN-5176433

The complaint

Mr B complains about Bank of Scotland plc trading as Halifax.

He says that Halifax didn't do enough to protect him when he fell victim to a scam, and would like it to refund him the money he has lost.

What happened

Mr B was scrolling through social media when he came across and advert for cryptocurrency supposedly being promoted by a well-known celebrity.

Mr B was persuaded that the involvement of a well-known business expert meant that there wouldn't be any risks involved and so registered his details through the ad and was taken to the company's website.

The website seemed professional and genuine. After registering his details, he received a call from someone that was to be his 'account manager'. They explained how he could make money from investing in crypto, and showed him how to use the system, including getting his profits back.

Mr B says that he looked up the website and was pleased to find positive reviews. So, he began to make payments, the majority of which was funded by a loan. I have set out the payments below – which were made to a payment processor via open banking, with which Mr B held an account.

Payment	Date	Payee	Payment type	Amount
1	07/09/2023	P	Faster payment	£1,500
2	14/09/2023	P	Faster payment	£4,250
3	04/10/2023	P	Faster payment	£1,000
4	10/10/2023	P	Faster payment	£3,500
			Total	**£10,250**

Mr B realised he had been scammed when he kept being pressured to pay more and more money, but he refused to do so, and the scammer cut contact with him.

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've decided not to uphold this complaint, for broadly the same reasons as our Investigator. I know this will be disappointing for Mr B, so I'll explain why.

In broad terms, the starting position at law is that banks and other payment service providers (PSP's) are 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. And I have taken that into account when deciding what's fair and reasonable in this case.

Mr B authorised the payments in question here – so even though he was tricked into doing so and didn't intend for the money to end up in the hands of a scammer, he is presumed liable in the first instance.

But this isn't the end of the story. As a matter of good industry practice, Halifax should also have taken proactive steps to identify and help prevent transactions – particularly unusual or uncharacteristic transactions – that could involve fraud or be the result of a scam. However, there is a balance to be struck: banks had (and 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.

Taking into account the law, regulator's rules and guidance, relevant codes of practice and what I consider having 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 that its customers were at risk of fraud (among 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.
- Have 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, 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.
- Have 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 case, I need to decide whether Halifax acted fairly and reasonably in its dealings with Mr B when he authorised payments from his account or whether it could and should have done more before processing them.

Having considered the payments Mr B made as part of the scam, I don't think that any of the payments in question would have alerted Halifax to the possibility Mr B may have been falling for a scam or at risk of financial harm. They payments were spread out and made via open banking to an account in his own name, and while payments two and four were relatively high, I can't see that there would have been any information available for Halifax to have known that they were ultimately being used to purchase crypto, only that he was making payments to an account in his own name. So, I don't think that Halifax needed to get in touch with him about what he was doing and why.

I am very sorry that Mr B has lost money to a scam and has found himself in debt as a result. However, the loss he has suffered has ultimately been caused by the scammer, not Halifax. And I can't ask Halifax to refund him when I don't think that it has done anything wrong.

My final decision

I don't uphold this complaint.

Under the rules of the Financial Ombudsman Service, I'm required to ask Mr B to accept or reject my decision before 16 April 2025.

Claire Pugh
Ombudsman