

## **The complaint**

Miss B complains that Bank of Scotland plc trading as Halifax ('Halifax') won't refund her after she was the victim of a scam.

## **What happened**

Miss B is represented in this case but for ease I'll refer to Miss B throughout this decision.

Miss B says that prior to the scam she had been following someone who specialised in trading and investments on social media. I'll refer to this person as H in my decision. Miss B felt that H was legitimate because she had numerous followers including celebrities. In November 2021 Miss B sent a message to H to say that she was interested in the cheapest investment scheme advertised by H. Miss B was told that if she invested £750, she'd receive £1,000 back within a week. She felt this was a reasonable rate of return and decided to go ahead on 12 November 2021.

H asked Miss B to open an account with a cryptocurrency exchange to exchange her funds for Bitcoin that she could send on to a wallet as directed by H so that H could complete trades on Miss B's behalf. Soon after she'd made the initial transfer Miss B was told she had made huge profits and agreed to withdraw her funds, but H told her she would need to pay £2,500 as an administration and withdrawal fee. After she'd made this payment Miss B was advised that she needed to pay £1,500 to cover tax as she had made so much profit. Miss B made all three payments over the course of around five hours.

Miss B realised she was the victim of a scam when H asked for more money, started to be rude to her and then blocked all contact. Miss B says she called Halifax to raise a scam claim on the day of the scam, but the wait was too long. She spoke to Halifax on 25 November 2021.

Halifax noted that the Lending Standards Board's Contingent Reimbursement Model Code (CRM Code) doesn't apply in this case as it only applies to payments to another person and the transactions Miss B disputes were to an account in her own name. Halifax also said that at the time the payments were made it had no concerns about them.

Miss B was unhappy with Halifax's response and brought a complaint to this service. She said Halifax failed to provide warnings in respect of the highly unusual transactions she had made so it should refund her in full and pay £500 compensation.

### *Our investigation so far*

The investigator who considered this complaint didn't recommend that it be upheld. She said that the transactions Miss B made weren't unusual enough to warrant intervention by Halifax and that Miss B had previously moved funds from her savings account to her current account before making payments, as she did on the day of the scam.

Miss B didn't agree with the investigator's findings. In summary, she said Halifax should have intervened when the payments were made because the payments were unusual in value and were made in quick succession - following a known pattern of fraud. Previous spending on the account was generally low with most payments not exceeding £200. Miss B also said that the transfers of £1,100 and £2,700 in September and October 2021 were to accounts in her own name and so shouldn't be taken into account. Finally, Miss B referred to

“BSI: PAS 17271: 2017 Protecting customers from financial harm as result of fraud or financial abuse” code of practice.

### **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.

In broad terms, the starting position in law is that Halifax is expected to process payments and withdrawals that a customer authorises it to make, in accordance with the terms and conditions of the customer’s account. It’s not disputed that Miss B made and authorised these payments, although I accept that at the time, she didn’t know she was being scammed.

However, taking into account the law, regulator’s rules and guidance, relevant codes of practice (including the BSI code I referred to above) 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 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.
- 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.

In this case, I need to decide whether Halifax acted fairly and reasonably in its dealings with Miss B when she authorised payments from her account or whether it could and should have done more before processing them.

I’ve seen evidence from Halifax that when Miss B made the first payment of £750, she was asked to provide the reason for the payment and was given a warning that was tailored to the payment purpose. Miss B said the payment was for an investment and was provided with a warning that said,

*“[name] make sure this investment is real*

- *Deals that look too good to be true can be scams.*
- *Do lots of research – good deals don’t find you.*
- *See what your family and friends think.*
- *Use the FCA to check an advisor or company.*
- *Find out how to stay safe from scams on our Fraud Hub.”*

There were links to the FCA website and to Halifax’s Fraud Hub.

After carefully considering this warning and Miss B’s statements for the twelve-month period before the scam I’m satisfied that Halifax did enough when Miss B made the scam payments.

I don't consider that the scam transactions were so unusual and out of character that Halifax ought reasonably to have done more than provide an on-screen warning when they were made. The amounts were relatively low, and Miss B has previously made payments to a different cryptocurrency exchange, so the payee wasn't unusual either. For example, in May 2021 Miss B transferred £1,000 from her Halifax account to a different cryptocurrency exchange and shortly before the scam transactions there were two £500 transactions on the same day to a cryptocurrency exchange. And the pattern of transactions didn't match common investment scams which involve payments increasing in value over time. In the circumstances, I don't consider the transactions Miss B made on 12 November 2021 would have caused Halifax any concern.

I appreciate the overall loss is significant to Miss B, but a balance must be struck between Halifax identifying potentially fraudulent payments, and responding appropriately to any concerns, and minimising disruption to legitimate payments. If all low value transactions such as the ones Miss B made in November 2021 were flagged by a bank for additional checks many legitimate payments would be affected.

As I am not upholding Miss B's complaint it follows that I am not awarding compensation.

Overall, whilst I'm very sorry to hear Miss B has lost money in a cruel scam, I can't reasonably ask Halifax to refund her loss.

### **My final decision**

For the reasons given, I do not uphold this complaint.

Under the rules of the Financial Ombudsman Service, I'm required to ask Miss B to accept or reject my decision before 6 November 2023.

Jay Hadfield  
**Ombudsman**