DRN-4939619

The complaint

Mrs E complains about Bank of Scotland plc trading as Halifax.

She says that Halifax didn't do enough to protect her when she became the victim of a scam and would like it to refund her the money she has lost as a result.

What happened

Mrs E received a phone call from a scammer who was pretending to be from Halifax's fraud team.

The scammer told Mrs E that her account had been compromised, and that she needed to send money to a safe account with R (a money remittance service) to protect her funds.

Mrs E complied with the request and made the following payments to R on 10 October 2023 via open banking.

- £3,490.00
- £4,981.99
- £6,981.99
- £991

At some point, the line went dead, and Mrs E realised she had been scammed. She reported this to Halifax and made a complaint.

Initially, Halifax declined her complaint – however, it later revisited this, and refunded Mrs E 50% of the last three payments (plus interest).

Mrs E remined unhappy and brought her complaint to this Service.

Our Investigator looked into things and thought that what Halifax had done was fair. They said that the initial payment wasn't significantly unusual or suspicious enough for Halifax to have had concerns that Mrs E was being scammed, and so Halifax didn't miss an opportunity to intervene.

However, they also said that Halifax was correct in identifying it could have done more with the subsequent payments. They said that refunding Mrs E 50% was fair, as Mrs E hadn't been as careful as she should have been before agreeing to make the payments.

Mrs E asked for a final decision, so the complaint .has been passed to me.

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 have decided that Halifax doesn't need to do any more than it already has, for broadly the same reasons as our Investigator.

I know this will be disappointing for Mrs E, 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.

Mrs E authorised the payments in question here – so even though she was tricked into doing so and didn't intend for the money to end up in the hands of a scammer, she 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.

Halifax has already agreed that it didn't do as much as it should have done to protect Mrs E from the scam – so the purpose of my decision is to decide if Halifax's has already done enough to put things right – and I think that it has.

Looking at the first payments Mrs E made, I agree that it wasn't sufficiently unusual or suspicious enough for Halifax to have had concerns that Mrs E may have been falling victim to a scam – while it may have been fairly large, it was going to a legitimate remittance

service, so there would not have been any concerns that the payment was going to anywhere which may have carried a higher risk, and it isn't unusual for individuals to make slightly higher one off payments on occasion.

I agree that when Mrs E made the second payment, less than forty minutes after the first was made, Halifax should have stepped in – which it has already admitted.

So, what is left for me to decide is if it is fair for Halifax to apply a 50% deduction for payments two to four to the refund it has already paid Mrs E.

Having considered what took place, I think that Halifax was fair to do so, as I don't think Mrs E was as careful as she should have been before agreeing to move money as instructed by the scammer.

While I understand that Mrs E was panicked by the phone call, I also think that there were several red flags that Mrs E ignored;

- The phone calls that took place came from a personal mobile number – not a recognised number of Halifax, which I think Mrs E could have verified, and while the scammer appears to have known some information about Mrs E, I don't think that a financial institution would contact a customer from a personal mobile number

- The scammer told Mrs E that her accounts with E-merchants A and E had been compromised, and by extension her account with Halifax. I don't think it is plausible that Halifax would be aware of any compromised accounts held with E-merchants.

- The use of R as a remittance service (with which Mrs E was instructed to open an account with) also does not seem plausible to me, and I find it unlikely Halifax would instruct a customer to move money to a different financial institution

- Mrs E was instructed to move the money in several payments, rather than one payment, and I can't see that it was explained to her why this would need to be done, if she was speaking to her genuine bank.

I have also considered if there was anything Halifax could have done to recover Mrs E's money, but I don't think there was. Mrs E confirmed that the money was moved on from R, so even if Halifax had contacted R immediately, then there would have been nothing for it to recover.

I am very sorry for the situation Mrs E now finds herself in, I know she has lost a lot of money and is rightfully upset by what has happened. But her loss wasn't caused by Halifax – it was the scammer that took her money, and I am satisfied that Halifax has already done enough to rectify its failings.

My final decision

Bank of Scotland plc trading as Halifax has already done enough to put things right for Mrs E, I don't direct it to do anything more.

Under the rules of the Financial Ombudsman Service, I'm required to ask Mrs E to accept or reject my decision before 6 May 2025.

Claire Pugh
Ombudsman