DRN-5052803

The complaint

Mrs K complains that Bank of Scotland plc trading as Halifax (Halifax) won't refund money she lost in an investment scam.

What happened

What Mrs K says:

Mrs K says she was introduced to investing with a firm ('firm A'). Her friend said it was easy and she was making money.

Mrs K set up a crypto wallet in her name and from there, sent money to firm A.

But when she tried to have her money repaid, she couldn't and she realised this was a scam – her friend had the same experience.

Mrs K says Halifax should've done more to protect her. Firm A had a warning against them on 23 March 2021 – and Halifax should've intervened in the payments and seen this. Had Halifax done so, the payments would've been stopped and Mrs K says she wouldn't have lost her money. She says Halifax should refund the money and pay compensation of £1,000.

The payments were:

Date	Payment	Amount
3 March 2022	Debit card to Mrs K's crypto wallet	£159.71
7 March 2022	Debit card to Mrs K's crypto wallet	£637.20
8 March 2022	Debit card to Mrs K's crypto wallet	£8.31
13 April 2022	Debit card to Mrs K's crypto wallet	£76.92
24 November 2022	Debit card to Mrs K's crypto wallet	£74.06
Total		**£956.20**

What Halifax said:

Halifax declined Mrs K's complaint and said:

- They spoke to Mrs K about one of the payments and she was adamant she wanted to go ahead.

- She said she'd done her checks.

- The payments were going to her own account – her crypto wallet and so they made the payments.

- Mrs K properly authorised the payments.

- The Contingent Reimbursement Model (CRM) Code didn't apply as the payments were made by debit card and the Code only covers faster online payments.

Our investigation so far:

Mrs K brought her complaint to us. Our investigator didn't uphold it as:

- The payments were in line with Mrs K's normal account activity.

- The payments were low in value.

- So, she said Halifax couldn't have been expected to intervene.

- On the call on 3 March 2022, Halifax spoke to Mrs K – but she said she'd done all her checks on the investment to make sure it was legitimate. She sounded confident and wanted it to go through.

Mrs K asked that an ombudsman look at her complaint and so it has come to me to make a final 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.

I'm sorry to hear that Mrs K has lost money in a cruel scam. It's not in question that she authorised and consented to the payments in this case. So although she didn't intend for the money to go to a scammer, she is presumed to be liable for the loss in the first instance.

So, in broad terms, the starting position at law is that a bank is 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 is fair and reasonable in this case.

But that is not the end of the story. Taking into account the law, regulators 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 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 make 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.

I need to decide whether Halifax acted fairly and reasonably in its dealings with Mrs K when she made the payments, or whether it should have done more than it did. I have considered the position carefully.

The Lending Standards Board Contingent Reimbursement Model Code (CRM Code) provides for refunds in certain circumstances when a scam takes place. But – it doesn't apply in this case. That is because it applies to faster payments made to another UK beneficiary– and in this case, the payments were made by debit card, and to Mrs K's account – her crypto wallet.

And while I accept this was a lot of money to Mrs K, the payments in question were in fact fairly low value ones. There was also nothing else about the payments that ought reasonably to have concerned Halifax.

There's a balance to be struck: Halifax has certain duties to be alert to fraud and scams and to act in their customers' best interests, but they can't be involved in every transaction as this would cause unnecessary disruption to legitimate payments. In this case, I think Halifax acted reasonably in processing the payments.

In this respect, I can see Mrs K made several other payments of a similar size to the largest scam payment of £637.20. So - this couldn't be seen as unusual.

Mrs K has argued that Halifax should've known the payments were going to firm A – and there had been a warning about firm A on the Financial Conduct Authority (FCA)'s website in March 2021. But here, as I don't consider Halifax had cause or a duty to intervene (for the reasons given) – they couldn't have been in a position to advise Mrs K not to make the payments.

On one occasion (3 March 2022), there was a call between Halifax and Mrs K. I listened to the call – Mrs K called Halifax to question why she had had a number of retail payments stopped. They mostly related to online purchases. The call handler resolved this by resetting Mrs K's debit card. Within the conversation, it came to light that three payments to the crypto wallet had also been stopped as part of this problem. The amounts were between euro191 and euro768.01.

Halifax's call handler asked Mrs K if she had done all the checks to make sure the investment was legitimate. Mrs K said she had. The call wasn't about payments to the crypto wallet being stopped for fraud checks – it was about an issue with Mrs K's card. Having said that, because Mrs K said she had done her checks – I don't think Halifax needed to do more. Given the relatively low sums of money involved, the conversation was proportionate to the amount of the payments.

Recovery: We expect firms to quickly attempt to recover funds from recipient banks when a scam takes place. I looked at whether Halifax took the necessary steps in contacting the bank that received the funds – in an effort to recover the lost money. Halifax told us there's no record that they attempted any recovery of the money.

But in this case, the funds went from the bank account to a crypto currency merchant and the loss occurred when crypto was then forwarded to the scammers. In this case, as the

funds had already been forwarded on in the form of cryptocurrency there wasn't likely to be anything to recover.

I'm sorry Mrs K has had to contact us in these circumstances. I accept she's been the victim of a cruel scam, but I can't reasonably hold Halifax responsible for her losses.

My final decision

I do not uphold this complaint.

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

Martin Lord
Ombudsman