

The complaint

Miss C has complained that Bank of Scotland plc trading as Halifax won't refund money, she says she lost to a scam.

What happened

Miss C has said that she was introduced to an 'investment opportunity' by someone she met via a social media platform. Miss C says she feels Halifax should have taken steps to prevent the scam and has asked for a full refund.

The transactions were as follows:

Date	Payment type	Amount
23/01/23	Faster Payment	£2.00
23/01/23	Faster Payment	£501.00
24/01/23	Faster Payment	£503.00
24/01/23	Faster Payment	£3,005.00
15/02/23	Credit	£6.00
20/03/23	Faster Payment	£250
20/03/23	Faster Payment	£250
03/04/23	Faster Payment	£250
11/04/23	Faster Payment	£2,000
24/05/23	Faster Payment	£4,000
12/06/23	Faster Payment	£4,000
12/06/23	Credit	£4,000
12/07/23	Faster Payment	£4,000
14/07/23	Faster Payment	£250
Total		£15,005

Halifax has said that it isn't responsible for Miss C's loss and confirmed that it intervened during one of the transactions and was satisfied with the explanations provided by Miss C. And as the payments were made to an account in Miss C's own name the complaint doesn't fall within the scope of the Contingent Reimbursement Model (CRM) Code.

Miss C was unhappy, so she brought her complaint to our service. Our investigator looked into her complaint but didn't recommend it be upheld. Miss C remained unhappy and for her complaint to be passed to me to consider.

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 agree with the investigators' findings for broadly the same reasons. I will explain why.

In broad terms, the starting position in law is that a bank is expected to process payments that their customer authorises them to make. It isn't disputed that Miss C knowingly made the payments from her account and so, I'm satisfied she authorised them. Therefore, under the Payment Services Regulations 2017 and the terms of her account, Halifax is expected to process Miss C's request, and she is presumed liable for the loss in the first instance.

However, taking into account the regulatory rules and guidance, relevant codes of practice and good industry practice, there are circumstances where it might be appropriate for Halifax to take additional steps or make additional checks before processing a payment to help protect customers from the possibility of financial harm from fraud.

The question then arises whether Halifax ought reasonably to have held such suspicions or concerns in relation to Miss C's payments - and if so, what might've been expected from a proportionate intervention at that time. Further to that, where there is an interaction between a customer and a bank before a high value payment is processed, as there was here, I'd expect the bank to take reasonable steps to understand the circumstances of that payment.

So, taking all of this into account, I need to decide if Halifax acted fairly and reasonably in their dealings with Miss C when she made the payments. Specifically, whether they should've done more than they did before processing them – and if they had, would that have made a difference. I also need to decide if Halifax could've reasonably recovered the lost funds.

Miss C's representative has said that Halifax ought to have considered the fourth payment (made on 24 January 2023) of £3,005.00 as unusual or uncharacteristic and intervened, I don't agree. While I accept that the amount of money Miss C sent is clearly significant to her, this doesn't in itself suggest a heightened risk of fraud. I also acknowledge that the transactions were larger than usual for the account. But I am not persuaded this would have stood out as unusual or suspicious. I say this because due to the date the payment was made, the fact the money was sent to an account (an electronic money institution) in Miss C's own name and payments had previously been made to this account, I don't think this type of payment activity would've stood out to Halifax as high risk in nature, whereby it gave it sufficient reason to suspect Miss C could be falling victim to a scam.

The payments which followed (between 15 February and 11 April 2023) were either low value payments (ranging between £250 and £2,000) or credits. The payments being disputed here were, individually, of a relatively low value. Although Miss C typically used her Halifax account for low value day to day transactions, she'd made payments of a similar or greater value in the prior 12 months. Because of this, I don't think the individual value of the payments would've been seen by Halifax as being unusual or out of character for Miss C.

Halifax has a difficult balance to strike in how it configures its systems to detect unusual activity or activity that might otherwise indicate a higher than usual risk of fraud. There are many millions of payments made each day, and it would not be possible or reasonable to expect a bank to check each one. As I mentioned above, while I don't doubt the payments represented a lot of money to Miss C, they are of values which I don't think would have appeared so suspicious or unusual to Halifax, when compared with other payments that it

processes daily. So overall I don't consider the payments Miss C made to have been remarkable enough to have warranted Halifax to act and have contacted Miss C ahead of processing them.

On 24 May 2023 Miss C made a payment of £4,000 to a cryptocurrency provider, this was also a larger payment that had debited the account in the previous six months. Therefore, in my view, there was enough about the characteristics of this transaction (taking into account when the payment was made) and the activity on Miss C's account that ought to have been concerning; such that Halifax should have intervened at that time to indicate she could be at risk of fraud. So, I am satisfied that it is fair and reasonable to conclude that Halifax should have warned its customer before this payment went ahead.

To be clear, I do not suggest that Halifax should provide a warning for every payment made to cryptocurrency provider. Instead, as I've explained, I think it was a combination of the characteristics of this payment (combined with those which came before it) the previous activity on the account and the fact the payment went to a cryptocurrency provider, which ought to have prompted a warning as it carried an elevated risk of fraud.

Halifax didn't intervene on this payment. But I think it would have been proportionate at that time for it to have issued Miss C with a written cryptocurrency warning. As, the information which would have been available to Halifax at that time, is that the transactions was of a certain value, being sent to a cryptocurrency provider.

However, I have considered what I think is likely to have happened if it had done so. From the evidence provided, it appears that Miss C had cryptocurrency experience. She was also very aware that she was 'investing' in cryptocurrency. As such I am satisfied that a cryptocurrency warning, wouldn't have alerted Miss C to the fact that she could be at risk of financial harm. This is also supported by the events that followed, which I will explain.

On 12 June 2023 Miss C attempted to make a transfer of £4,000 to another cryptocurrency provider. Halifax identified the payment as potentially suspicious and blocked the payment and asked Miss C to contact it. I have reviewed the transcript from the call which took place that day. Miss C's representative has said the intervention wasn't sufficient as Halifax should have asked open and probing questions to establish the circumstances and risk around the payment. And while, I wouldn't have determined this payment warranted human intervention, Halifax did, as such I have considered how affective Halifax's intervention was.

Having reviewed the transcript I can see Miss C explained that she was purchasing cryptocurrency through her Ledger wallet and explained that she trusted and felt it was a secure platform. However, Miss C was asked if anyone had recommended this 'investment' (on two occasions) and she confirmed no. This directly contradicts what Miss C's representative has told our service. Miss C's rep said that she had met someone on social media who "persuaded her to invest in crypto and was advised on specific trade" Therefore, I don't agree that Miss C answered the advisors' questions in the spirit they were intended and by denying the advisor the opportunity to know that there was a third party who recommended the investment and was giving Miss C advice on specific trades, denied them the opportunity in identify the potential risk Miss C faced.

While I accept Miss C's representative has highlighted that the advisor didn't go far enough in asking open and probing questions to unveil the scam, even if I agreed, I am not convinced, even if the advisor had done so, Miss would have provided accurate answers to the questions she was asked. Therefore, I don't agree the scam would have been uncovered. Therefore, I can't reasonably hold Halifax responsible for this.

Recovery

I have gone on to consider if Halifax took reasonable steps to try and recover the funds once it was made aware. Miss C didn't make the payments to the scammer directly; she transferred her funds to an account in her own name. If these funds had not already been transferred to the scammer they would be in her control to access as and when she chose. Halifax would not have been able to attempt to retrieve the funds from the scammer directly as that is not where the funds were originally sent to. So, it follows that I won't be asking Halifax to do anything further.

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 Miss C to accept or reject my decision before 12 November 2025.

Jade Rowe
Ombudsman