DRN-5154220

The complaint

Miss M complains that Bank of Scotland Plc trading as Halifax ("Halifax") won't refund her multiple payments made from her account as the result of an investment scam.

What happened

In February 2023, Miss M was involved in a scam. She was persuaded to send £3,450, over a series of payments, from her Halifax account to someone who said they would be able to mine/invest in cryptocurrency on her behalf. Unfortunately, we now know this person to be a scammer.

Miss M had seen the investment opportunity being recommended by one of her friends on her social media profile and so she thought the investment was genuine. However, unbeknown to Miss M at the time, her friend's profile had been hacked by scammers.

It's not clear how the investment was supposed to work but Miss M was told that if she invested an initial amount of £500, she would get £10,050 in return within 3 hours of investing. However, when Miss M asked to withdraw her funds she was told she would need to pay various additional fees that were required to release her 'profits'. After continuing to make further payments and still not seeing any returns, Miss M eventually realised she'd been scammed. Miss M then contacted her bank for help.

Halifax looked into Miss M's complaint, but it didn't offer her a refund of the funds she had lost. It said it had contacted the scammers bank in relation to the first payment Miss M had made, but it hadn't been able to retrieve any her funds. Halifax went on to say that it would not look to assume liability for Miss M's overall losses and offer her a refund now.

Unhappy with Halifax's response, Miss M brought her complaint to our service. One of our investigators looked into things, but they didn't uphold the complaint.

They said they didn't think Miss M had a reasonable basis for believing that the investment she had entered into was genuine. Specifically, they said the returns she had been promised were too good to be true and Miss M hadn't done enough checks before entering into the investment. They also didn't think that the payments Miss M had made during the course of the scam were so unusual that Halifax needed to intervene and speak with Miss M prior to processing them on her behalf, they were in line with Miss M's usual spending on the account.

Miss M disagreed and as an informal agreement could not be reached the case has been passed to me for 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.

Having done so, I agree with the findings put forward by our investigator and I won't be asking Halifax to take any further action. I'll explain why in more detail below:

The CRM Code

The first payment that left Miss M's account was made via faster payment and went directly to an account controlled by the scammer. This means it is covered by the provisions of the Lending Standards Board Contingent Reimbursement Model ("the CRM code") which requires firms to reimburse customers who have been the victims of Authorised Push Payment ("APP") scams like this, in all but a limited number of circumstances.

A customer who has fallen victim to a scam should, under the CRM Code, be refunded in full in most circumstances. But the Code does set out exceptions to reimbursement which a business can choose to rely on, if it can evidence that they apply. Halifax has said that one such exception applies in Miss M's case. Halifax says that:

- Miss M lacked a reasonable basis for believing she was dealing with a legitimate person for legitimate purposes.

It is then for me to decide whether this exception to reimbursement can be fairly relied on.

It is not in dispute that Miss M has been the victim of a cruel scam. I'm satisfied the proposition offered by the scammer was a fraudulent scheme. But I then need to consider the merits of Miss M's individual case, taking into account her specific circumstances.

Did Miss M have a reasonable basis for belief when she made Payment 1?

For clarity, I'm only considering Miss M's basis for belief in relation to the first payment as the remainder of the payments that left Miss M's account are not covered by the CRM Code.

Taking into account all of the circumstances of this case, including the characteristics of Miss M and the complexity of the scam, I think the concerns Halifax have raised about the legitimacy of the transaction Miss M made are enough to support its position that it wasn't reasonable for Miss M to have believed what the scammer was telling her.

I don't think Miss M had a reasonable basis for believing the scammer was the person they held themselves out to be or that the investment on offer here was genuine. In reaching this conclusion I have taken into account the following:

- Miss M became involved in the proposed investment after a very brief conversation with someone over a text messaging service - which is not a method used to arrange and agree legitimate investments. The scammer also asks Miss M to lie about the reason she is making the payment when entering the payment details, which isn't something a genuine financial professional would do. I therefore think that the nature of the messages, in combination with the other factors, ought reasonably to have led Miss M to have concerns.
- I haven't seen any evidence of a contract or any other documentation signed by Miss M and the scammer that would indicate she was entering into a genuine investment.

- The investment Miss M was offered did not sound genuine and it's unclear how the investment was supposed to work or how it could generate such large profits in such a short period of time.
- The rate of return Miss M was offered and the timescale to receive it were too good to be true. Miss M was told to invest £500 and she would receive a return of £10,050 within a 3-hour period. These rates of return are not plausible. And so, I'm satisfied that the rate of return being offered here was so unrealistic and so unlikely that Miss M ought reasonably to have had significant concern about the legitimacy of the opportunity that was presented to her. That, in turn, ought to have led to a greater degree of checking on her part.
- Miss M doesn't appear to have carried out any checks on the scammer before she agreed to make the payments and she didn't do anything to verify the scammer was who they said they were. And so, at the point Miss M agreed to invest, she was essentially making payments to an unverified stranger online.

So, overall, I'm not persuaded that it was reasonable for Miss M to have believed she was entering into a genuine investment. And I don't think she completed enough research before deciding to go ahead and invest - particularly given the significant red flags in this case.

Did Halifax need to provide Miss M with an effective scam warning in regard to payment 1?

The CRM Code also sets out standards for firms – that is, what firms are expected to do to protect customers from the risk of fraud and scams. One of those requirements is that, where the firm has (or should have) identified that its customer is at risk from a scam, it should provide that customer with an "effective warning", within the meaning of the CRM Code.

Payment 1 amounted to £500. So, it was relatively low in value, and I don't think it was remarkable enough to have stood out to Halifax as an APP scam risk. Overall, I don't think there was anything so suspicious about the payment that would've indicated to Halifax that it was being made as a result of an investment scam. So, I'm not persuaded that the bank needed to provide Miss M with an effective warning or that Halifax has failed to meet its obligations under the CRM Code. Because of this, I won't be recommending that Halifax provide Miss M with a refund of this payment now.

Payments 2, 3 and 4

Payments 2, 3 and 4 initially went to an account in Miss M's own name and so they are not covered by the provisions of the CRM Code.

It is accepted that Miss M authorised these payments herself. So, although she didn't intend the money to go to scammers, under the Payment Services Regulations and the terms and conditions of her account, Miss M is presumed liable for her loss in the first instance.

Where a valid payment instruction has been received, Halifax's obligation is to follow the instructions that Miss M has provided. However, there are circumstances where it might be appropriate for Barclays to take additional steps or make additional checks before processing a payment in order to help protect its customers from the possibility of financial harm from fraud. An example of this would be when a payment is sufficiently unusual or uncharacteristic when compared with the usual use of the account.

In such circumstances, I'd expect Halifax to intervene and ask some questions about the intended payment(s) before processing. So, I've first thought about whether the payments

Miss M made could be considered out of character and unusual when compared with her usual account activity.

I've reviewed Miss M's account statements for the months leading up to the scam, and I don't think the payments were remarkable enough for them to have stood out to Halifax and to have prompted further discussion. I'll explain why:

Payments 2, 3 and 4 amounted to £1,150, £1,250 and £550 and they were made multiple days apart.

The payments are all for relatively modest amounts and they aren't inherently suspicious when considering that it is quite common for customers to process transactions up to this amount on a daily basis. Miss M had made payments that were similar in value in the preceding months.

So, overall, I'm not satisfied that the scam payments should have stood out or looked so unusual when compared to Miss M's genuine account activity that they should've prompted further checks by Halifax before they were allowed to leave her account.

I have to stress that, at the time, Halifax wouldn't have known that Miss M was making payments at the request of a scammer. It is now only with the benefit of hindsight that we know that the payments were being made as the result of a scam. Banks have to strike a balance between processing payments as per their customer's instructions and monitoring accounts for unusual and potentially harmful activity. And I don't think it would be fair to say that Halifax should've identified the payments Miss M made as suspicious enough to warrant further checks.

I've also thought about whether Halifax could've done more to help Miss M once it was notified of the scam but I don't think it could. The funds sent as part of the first payment had already been removed from the receiving account and the remaining funds had also already been moved on from Miss M's account to the scammer - so there wasn't anything Halifax could've done to recover the funds.

Finally, I want to say again that I am very sorry to hear about what has happened to Miss M. I have significant sympathy for the situation she has found herself in. But at the same time, I don't think her loss was caused by any specific failing on behalf of Halifax. The fault here lies with the cruel and callous acts of the scammers themselves.

My final decision

My final decision is that I do not uphold this complaint.

Under the rules of the Financial Ombudsman Service, I'm required to ask Miss M to accept or reject my decision before 28 July 2025.

Emly Hanley Hayes
Ombudsman