DRN-5690384

The complaint

Mrs M complains that Bank of Scotland plc, trading as Halifax, won't refund the money she lost to an investment scam. Mrs M is represented in this complaint, but I'll refer to her as it's her complaint.

What happened

The detailed background to this complaint is well known to both parties. So, I'll only provide a brief overview of some of the key events here.

On social media, scammers were posing as a legitimate investment through fake Company R.

Mrs M explains that she saw the Company R advertisement which seemed highly successful and showed she could make amazing amounts of money and after completing due diligence, which included online checks, she signed up to their special two-week investment programme.

Mrs M says she was given further confidence by the scammers as their website connection appeared to be linked to a genuine crypto exchange. Also, she thought she was part of a group of other investors who confirmed they had been successfully withdrawing their funds from the platform.

Mrs M was referred to a professor and his assistant who provided trading signals up to three times a day at set times. They advised her to increase her deposits and told her that she would need to pay 15% commission on her profits.

Mrs M made the following payments to the scammers after crediting her Company C crypto exchange account:

Payment Number	Date	Payment Method	Beneficiary	Amount
1	3 October 2024	Debit card	Mrs M's account with Company C	£848.52
2	18 October 2024	Debit card	Mrs M's account with Company C	£824.98
3	19 October 2024	Debit card	Mrs M's account with Company C	£1,220.34
4	26 October 2024	Debit card	Mrs M's account with Company C	£2,045.57
5	26 October 2024	Debit card	Mrs M's account with Company C	£2,045.57
6	26 October 2024	Debit card	Mrs M's account with Company C	£2,045.57
Total				£9,030.55

Mrs M thought she was trading 'up to 30X the initial amount' (making around £270,000 from her total investment of around £9,000) and requested a withdrawal. But she was asked to pay a large fee, which couldn't be deducted from her account, and it then dawned on her that she'd been scammed.

Mrs M complained to Halifax seeking a refund, interest and compensation of £1,000 for the trouble and upset caused. Mrs M said:

- *'At no point did the bank get me to check or verify why I was putting so much money into a crypto so fast. I have never put any more than a few hundred into Crypto and not for many many years (previously the last time was around 2018 I think). I've had banks stop me from paying for anything more than a thousand many times in the past to check that I really knew why and for what reason. I've often found these annoying but in this case, it would have been helpful and yet when it was much more needed, it was not done'.*

Halifax declined her refund request, saying the Contingent Reimbursement Model (CRM) code didn't apply due to the payments being made by card and they didn't have any rights to try and get the money back using the chargeback scheme.

Mrs M was dissatisfied with Halifax's response and brought her complaint to our service. Our investigator said Halifax should've intervened at payment number 5 and thought it likely this would've unravelled the scam. She also considered there was contributory negligence from Mrs M. So, she said Halifax should pay 50% of Mrs M's loss from payment 5.

Mrs M agreed but Halifax didn't. Halifax's reasons include the following:

- Mrs M's payments weren't unusual or out of character as:
    - Approximately two weeks before payment 1 (on 16 September 2024), Mrs M made four debit card payments on the same day, totalling £6,426.68, and one of these payments, for £600, was to another crypto exchange company (Company S).
    - Mrs M made further payments to Company S (for £200, £150 and £200) between payments 3 and 4 (on 23 October 2024), all in a one-hour period.
- Not all payments relating to crypto are made as a result of fraud or a scam and Mrs M was already investing in crypto. So, there is no reason to believe she would've disclosed she was moving the money out of the wallet on the advice of someone she met on social media.
- Although they don't disbelieve Mrs M lost money to a scam, they haven't seen evidence of her loss and note that she continued to credit / use her Company C account in 2025.

As Halifax disagree this complaint has been passed to me to look at.

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'm partially upholding this complaint and I'll explain why.

I should first say that:

- I'm very sorry that Mrs M has been the victim of this cruel investment scam and lost a significant amount of money here.
- Although I don't underestimate the severe impact this has had on Mrs M, I must approach this matter objectively.
- I've carefully considered all the points Mrs M and Halifax have made and I've focused on what I think are the important points to reach a final decision.

- I'm satisfied that the Contingent Reimbursement Model (CRM) and then the APP Scam Reimbursement Rules, introduced by the Payment Systems Regulator in October 2024, for customers who have fallen victim to an APP scam, don't apply here as the payments Mrs M authorised were by card to another account under her control.
- Regarding efforts to recover Mrs M's loss. As the payments to the scammer were sent to a crypto exchange and then onto the scammer, I don't think Halifax could've been expected to recover them. Also, unfortunately, it wouldn't have been possible for Halifax to raise a card chargeback claim as the rules don't cover scams.

It isn't in dispute here that, having been persuaded by the scammers, Mrs M authorised Halifax to make the payments in the above table. So, although she clearly didn't intend the money to go to a scammer, the starting position in law is that Halifax were obliged to follow their payment instruction and Mrs M isn't automatically entitled to a refund.

Under the Payment Services Regulations 2017 (PSR) and in accordance with general banking terms and conditions, banks should execute an authorised payment instruction without undue delay.

The starting position is that liability for an authorised payment rests with the payer, even where they are duped into making that payment. In accordance with the law, regulations and good industry practice, a bank should be on the look-out for and protect its customers against the risk of fraud and scams so far as is reasonably possible. If it fails to act on information which ought reasonably to alert a prudent banker to potential fraud or financial crime, it might be liable for losses incurred by its customer as a result.

However, banks do have to strike a balance between the extent to which they intervene in payments to try and prevent fraud and/or financial harm, against the risk of unnecessarily inconveniencing or delaying legitimate transactions.

I consider Halifax should at that time fairly and reasonably:

- Have been monitoring accounts and any payments made or received to counter various risks such as anti-money laundering and preventing fraud and scams.
- Have 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.

Also, from July 2023 Halifax had to comply with the Financial Conduct Authority's Consumer Duty which required financial services firms to act to deliver good outcomes for their customers. Whilst the Consumer Duty does not mean that customers will always be protected from bad outcomes, Halifax was required to act to avoid foreseeable harm by, for example, operating adequate systems to detect and prevent fraud.

With the above PSR and Consumer Duty in mind, I considered whether:

<u>Halifax should've identified that Mrs M was at risk of financial harm and put in place proportionate interventions?</u>

Payments 1 to 4

I wouldn't have expected Halifax to have been concerned about any of these four payments. This is because Mrs M had made payments to other accounts with companies that trade in crypto, the payments were for relatively low amounts, there weren't any suspicious high velocity payment patterns with most of the payments spread over a three-week period.

Also, crypto payments are both legal and common with banks like Halifax processing thousands of payments and, as mentioned above, they have a balance to strike when deciding whether to intervene.

In addition, although not specific to crypto payments Halifax would have some comfort in knowing that, prior to release of the payments, Mrs M would've received at least one automated general scam warning prompting her to check the legitimacy of the company she was paying and that the '*price isn't too good to be true'*.

Payment 5

Payment 5 for £2,045.57 was the second payment on 26 October 2025 and for the same amount as payment 4, which meant Mrs M was spending over £4,000 that day. This was much higher than any of the previous payments she had previously made to a crypto exchange.

I recognise there were days where Mrs M's total spend was higher and these included a payment to a crypto company, but that £600 crypto spend was much less. Also, there was a day where there were several crypto transactions made within one hour. However, the total crypto spend on that date was £550. And importantly, Halifax would be aware that crypto payments have an elevated risk, and their regulator says customers should be prepared to lose all their money. Also, many frauds and scams involve crypto payments.

So, I also think, prior to releasing payment 5, Halifax should've completed analysis, identified a risk and put in place an intervention with one of their fraud and scam agents to check that Mrs M wasn't at risk of financial harm.

If a bank doesn't question payments that might be at risk, then it can't fulfil its duty to protect customers. I'm not saying that means it must check every payment out of its customers' accounts. But here, considering the amount of the crypto payments on 26 October 2024, I believe it ought to have contacted Mrs M to check she wasn't at risk of falling victim to fraud.

I then considered what would've happened if Halifax had put in place a human intervention and whether, by not putting this in place, Halifax caused some of Mrs M's loss.

Causation

To do this, I looked closely at the information on file and reflected on whether this type of intervention would've made any difference.

I think a Halifax fraud and scam agent would've likely asked the following type of open questions and then probed Mrs M's answers to give her the best educational information, appropriate warnings and to try and detect a scam:

- Payment purpose.
- Expected returns and ability to withdraw.
- Contact method.
- Checks and research completed.
- Third parties, brokers or recovery agents advising of fees.
- Third party communications including requests to deceive the bank and download computer sharing software.

Having reviewed Mrs M's dialogue with the scammer, although she didn't tell the scammer about any bank interventions (because they didn't occur), I can't see any evidence of coaching (in advance of investment payments) to mitigate the risk of bank interventions.

Also, I can't see any comments showing she was anxious about her investment success being hampered or stopped. In addition, Mrs M was worried about not having made a withdrawal. So, although I can't be certain, I haven't seen any information to suggest Mrs M wouldn't have given honest answers to Halifax's questions.

Upon being asked probing questions, I think Mrs M would've explained the trading company, that she was being helped and guided and that she'd made high profits but hadn't yet made a withdrawal. I then think an agent would've quickly:

- Probed who the trading was with and how the trading was controlled.
- Looked up the company.
- Noticed it wasn't FCA approved and there was no footprint.
- Seen concerning comments about other companies with similar names.
- Given educational information on typical scams.
- Told Mrs M she was highly likely being scammed.

I think Mrs M would've then stopped the payment, made more enquiries, attempted a withdrawal and come to the same realisation. Also, I think the agent would've in the meantime blocked any further payments to Company C, preventing any further loss.

Having established that Halifax should've intervened and that this would've more likely than not uncovered the scam and prevented any further loss, I looked at:

<u>Contributory negligence</u>

I noted that our investigator looked closely at contributory negligence and thought it applied here. I also considered this as there's a general principle that consumers must take responsibility for their decisions.

Although I recognise how clever these cruel scammers are and in no way blame Mrs M for being scammed, I think she should've been more diligent before making the payments. Mrs M is understandably devasted by this scam and accepts the 50% deduction in a refund. Due to her acceptance and our investigator highlighting Mrs M should've done more research on the trading platform and returns which sounded far too good to be true, all of which I agree with, I won't further elaborate on contributory negligence.

Regarding Mrs M's request for a compensation payment, given Halifax ought to have prevented some of the loss from occurring. As distress and inconvenience has been caused by the cruel scammer, rather than Halifax, I don't think it would be fair and reasonable to require them to make a compensation payment here.

Finally, regarding Halifax's comments about Mrs M continuing to make payments to Company C and not having seen evidence of her loss, I can confirm that I've seen a Company C statement that correlates with her payments.

Putting things right

Having considered all the above, I think both Halifax and Mrs M are equally at fault here. Halifax should've put in place an intervention at payment 5, which would've likely unravelled the scam and stopped further payments, and Mrs M should've been more diligent. So, I think it is only fair and reasonable for liability to be shared.

So, my decision is to partially uphold this complaint, and I require Halifax to:

- Refund £2,045.57 (50% of payment 5 and payment 6).
- Pay 8% simple interest from date of loss to the date of settlement.

My final decision

For the reasons mentioned above, my final decision is to partially uphold this complaint against Bank of Scotland plc, trading as Halifax, and my requirements are detailed in the above putting things right section.

Under the rules of the Financial Ombudsman Service, I’m required to ask Mrs M to accept or reject my decision before 2 January 2026.

Paul Douglas
Ombudsman