DRN-5858694

The complaint

Mr R complains that Bank of Scotland plc, trading as Halifax, won't refund the money he lost to an investment scam. Also, he is dissatisfied with the service he received when he complained. Mr R is represented but I'll refer to him as it's his 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.

In September 2024, Mr R received an app message from an unknown number about a domestic emergency, and he told them they'd got the wrong number. He received more messages and engaged dialogue with Person H (the scammer), and they started to converse about crypto investments.

Mr R had an interest in investments as he had recently been diagnosed with a very serious health condition and was thinking about ways to generate income for his family.

Person H led him to believe that he could get a return on his investment of up to 50% and she told him about the significant profits that she'd made from a (fake) trading platform. She persuaded Mr R to start investing and helped him set up an account with Company C (a legitimate crypto company) so he could buy USDT and then transfer it to the trading platform via a crypto wallet that she controlled.

Person H showed Mr R illustrations of his trading success, and this encouraged him to make more and more payments to the trading platform.

Mr R took out two loans and after crediting his Halifax account he made the following payments, totalling £24,100, to Company C and then onto the fake trading platform:

Payment Number	Date	Payment Type	Payee	Amount
1	10/9/24	Faster Payment	Mr R's account with Company C	£200
2	11/9/24	Faster Payment	Mr R's account with Company C	£800
3	14/9/24	Faster Payment	Mr R's account with Company C	£1,000
4	17/9/24	Faster Payment	Mr R's account with Company C	£1,000
5	20/9/24	Faster Payment	Mr R's account with Company C	£1,000
6	24/9/24	Faster Payment	Mr R's account with Company C	£2,000
7	29/9/24	Faster Payment	Mr R's account with Company C	£700
8	4/10/24	Faster Payment	Mr R's account with Company C	£900
9	14/10/24	Faster Payment	Mr R's account with Company C	£7,000
10	18/10/24	Faster Payment	Mr R's account with Company C	£1,000

11	23/10/24	Faster Payment	Mr R's account with Company C	£1,000
12	25/10/24	Faster Payment	Mr R's account with Company C	£1,000
13	30/10/24	Faster Payment	Mr R's account with Company C	£6,300
14	4/11/24	Faster Payment	Mr R's account with Company C	£200
Credit				£83.09
Total loss				£24,016.91

In late October 2024, when Mr R thought he'd made a good profit, he tried to withdraw funds, but the scammer's system demanded a fee. Despite paying this, he still couldn't make a withdrawal, and he was then devasted to realise he had been scammed.

Mr R contacted Halifax to claim a refund, and they told him to contact Company C as that was the account he paid the scammer from.

Mr R subsequently brought a complaint to Halifax seeking a full refund, interest and a distress payment for originally refusing to consider a refund. He said that Halifax should've done more to warn him and prevent the scam particularly given the pattern and size of the transactions.

Halifax rejected his complaint and claim. They said that the payments weren't covered by the 'Contingent Reimbursement Model (CRM) code, or Payment Systems Regulator (PSR) mandatory reimbursement rules'. Also, they explained that they continuously monitor accounts, but his payments weren't out of character and were in line with his previous spending pattern.

Mr R was dissatisfied and brought his complaint to our service. Our investigator considered that Halifax should've recognised a risk of financial harm at payment 9 (for £7,000) and put in place a human intervention. He thought this would've likely unravelled the scam and stopped Mr R making further payments and said Halifax should provide a refund from payment 9. However, he said this should be 50% because of contributory negligence from Mr R.

Mr R accepted this view, but Halifax disagree. Halifax still don't think the payments were unusual and requested an ombudsman 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'm partially upholding this complaint, and I'll explain why.

I should first say that:

- I'm satisfied that Mr R was the victim of a cruel investment scam.
- I'm very sorry that Mr R has had this experience, in addition to his serious health condition, and lost a significant amount of money here.
- In making my findings, I must consider the evidence that is available to me and use it to decide what I consider is more likely than not to have happened, on balance of probabilities.
- I considered the CRM Code and APP fraud mandatory reimbursement rules, which require firms to reimburse customers who have been the victim of a scam in most

circumstances. However, these codes unfortunately don't apply due to Mr R sending the payments to another account he held.

- Regarding recovery, as Mr R's funds were passed on to a crypto company and then paid to the scammer's crypto account where they would've been emptied, I wouldn't have expected Halifax to have been able to recover his funds even if they immediately accepted his complaint.
- Regarding the service strand of this complaint, whilst I fully understand Mr R's frustrations at being told to speak to Firm C to obtain a refund, when considering how the payment was made and Halifax's position (stated in their final response letter), I don't think it was unreasonable of Halifax to respond in this way and this should warrant compensation.
- The Payment Services Regulations 2017 (PSR) and Consumer Duty are relevant here.

PSR

Under the 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. There's no dispute that Mr R made the payments here, so they are considered authorised.

However, 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.

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. So, I consider Halifax should 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 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 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.

Consumer Duty

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.

Also, it required them to look out for signs of vulnerability. Although I'm very sorry to hear about Mr R's serious health condition, I can't see that Halifax were aware of this and discussed risks and mitigation with Mr R.

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

Whether Halifax should've recognised Mr R was at risk of financial harm and put in place a proportionate intervention?

Although I recognise Company C is a legitimate company, that Mr R had previously made some large payments (higher than the largest payment in the above table) and it wasn't unusual for him to credit his account before making a payment, it is important to note the following:

- Halifax knew all the payments here were going to a well-known crypto company.
- Mr R hadn't previously made any crypto payments and only set up Company C as a payee from payment 1, when he was persuaded to do so by the scammer.
- The previous large payments (that exceeded £7,000) were 12 months previous and clearly not related to crypto. Also, they appear to have been one off mortgage payments and, having reviewed Mr R's statements, it was rare for him to make such large payments.
- From 2023, there had been widespread coverage in the media about the increase in losses to cryptocurrency scams and Halifax's regulator (the Financial Conduct Authority) had previously warned about the risks of cryptocurrency scams and that *'If consumers invest in these types of product, they should be prepared to lose all their money'.* So, Halifax should've therefore recognised that cryptocurrency related transactions carry an elevated risk of the likelihood of the transaction being related to a fraud or scam.

Considering the elevated risk here and that Mr R made 14 separate payments to a crypto company for £24,100 in an eight-week period, I would've expected Halifax to have completed analysis, recognised the risk and put in place proportionate interventions to provide education, warnings and to ask probing questions to detect a fraud or scam.

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 they were new and multiple crypto payments, I believe it ought to have contacted Mr R to check he wasn't at risk of falling victim to fraud. And Halifax haven't provided any evidence to show they did this.

I then considered:

When and how Halifax should've proportionately intervened

I think that upon payment 6, where high risk crypto payments were made with some frequency and higher than average spend (six being made in a two-week period totalling £6,000), a proportionate intervention would've been an automated warning about crypto and crypto investments.

Having considered Mr R's conversation with Halifax in June 2024 (which involved general scam education including scammers making unexpected contact by the same messaging app), his dialogue with the scammer who he'd started to trust and who had convinced him that he'd made a profit, I can't be confident that Mr R would've taken note of such an automated intervention and I think a human intervention would've been needed to stop him paying the scammer.

I wouldn't have expected any intervention on payment 7 and 8 as these were under £1,000 but payment 9 was for £7,000. Although there was a gap of three weeks between payment 6 and 9, this was a large payment for Mr R to make. As mentioned above, the large payments Halifax highlighted were a while back (September 2023) and weren't crypto and / or investment related. Also, from analysing Mr R's statements in the previous twelve months it was unusual for him to make such a large payment. In addition, the pattern of crypto payments mostly around £1,000 was suddenly significantly exceeded, which on high-risk crypto payments could be an indicator of a scam.

So, I agree with our investigator that at payment 9 Halifax should've put in place a human intervention.

I then considered:

What would've likely happened upon a human intervention call and whether this would've resulted in the scam being unravelled and prevented some of Mr R's loss

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

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

Having read Mr R's submissions and closely reviewed his daily dialogue with Person H, although there weren't any interventions for Person H to navigate and she mentioned the need for Mr R to make low amount payments to avoid intervention, there isn't any evidence of her telling him what to say in that event. Also, I noted how Mr R was assertive with Person H, keeping his banking including loan applications private and he didn't take note of her advice on the size of payments. So, I think, more likely than not, that he would've given open and honest answers to the above type of typical questions.

Upon being asked probing questions, I think Mr R would've been honest and explained the trading platform he was using, that he was being helped and guided and that he'd made some early profits but hadn't yet made a withdrawal. I then think an agent would've quickly:

- Become suspicious about who he was receiving help and guidance from.
- Probed how he met Person H.
- Probed who the trading was with and how the trading was controlled.
- Checked the trading platform and found it wasn't approved and there were concerning comments.
- Given educational information on typical scams and told Mr R she suspected he was being scammed.

I think Mr R would've then realised he'd been scammed or have stopped the payment and made more enquiries and come to the same realisation after attempting a withdrawal (knowing the scammer's release fee tactic). And, if the latter was the case, I think the agent would've in the meantime blocked that payment and further payments, 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:

Contributory negligence

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 Mr R for being scammed, I think he should've been more diligent before making the payments. Mr R is understandably devasted by this scam and accepts the 50% deduction in a refund. Due to his acceptance and our investigator highlighting Mr R should've done more research (on the

trading platform, Person H who was advising him and returns which sounded too good to be true), which I agree with, I won't further elaborate on contributory negligence.

Putting things right

Having considered all the above, I think both the business and customer are equally at fault here. Halifax should've put in place an intervention at payment 9, which would've likely unravelled the scam and stopped further payments, and Mr R should've been more diligent. So, I think it is only fair and reasonable for liability to be shared.

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

- Provide Mr R with a refund of £8,208.45 {50% of £16,416.91 which is payments 9 to payment 14 less the credit received of £83.09}.
- Pay 8% simple interest on the refund from the 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 Mr R to accept or reject my decision before 17 December 2025.

Paul Douglas
Ombudsman