

## **The complaint**

Mr S complains that Bank of Scotland plc trading as Halifax (Halifax) hasn't fully refunded him for the money he lost to what he now believes was an investment scam.

## **What happened**

Mr S holds both a current account and a savings account with Halifax.

Mr S explains that around 2020, a friend had mentioned an investment opportunity to him. He says he initially had doubts about it and decided not to pursue the investment at the time. But in 2021, Mr S's friend mentioned it again. His friend told him that they had a friend who'd invested and supposedly made profits.

Mr S was told he'd receive returns of 10% a month. His investment could be left to grow or withdrawn at a week's notice. He was promised his invested capital would be guaranteed – there was no risk.

Purportedly the trader had previous experience working in finance. He claimed to have been trading independently for some time. But because the trader was still in the process of setting up a company, payments needed to be made to his personal bank account. No brochures or documentation were available, and the trader didn't yet have a website but would be setting one up.

Mr S says he was provided with an investment contract. He says the initial version had the wrong investment amount, and he needed to return it to be corrected.

Trusting the recommendation of his friend and what he was told by the trader, on 14 April 2021 Mr S made an initial investment of £20,000. He says he paid for this from money in his savings account. Mr S sent these funds as a Faster Payments transfer from his current account to the personal account of the trader.

Mr S says he later sought to borrow money from his sister. She took out a personal loan in her own name and lent Mr S £15,000.

Mr S used £2,000 of the amount his sister had lent him for other purposes. But he invested the remainder of the money his sister had lent him. He did so through three further payments on 17 May 2021: two payments of £5,000, and one of £3,000.

In total, he'd invested the sum of £33,000.

Having invested, the trader sent Mr S a spreadsheet showing he was making profits on his investment. However, when Mr S later wanted to withdraw some of his money, he was told it would take a bit longer than had been initially promised. He was given further excuses, but no money was returned.

Eventually Mr S learned that many other people had also sent money to the trader and couldn't withdraw their money either. He was told that the trader had been reported to the

Police.

Mr S reported what had happened to his bank. He said he'd been the victim of an investment scam – an Authorised Push Payment Scam (APP Scam).

Halifax is a signatory of the Lending Standards Board's Contingent Reimbursement Model (the CRM Code). The CRM Code requires firms to reimburse customers who have been the victims of APP scams in all but a limited number of circumstances.

Halifax said it would partly refund Mr S, for the third and fourth payments he'd made (payments of £5,000 and £3,000). It said it could have done more to protect him at the point he'd made these payments. But it thought Mr S should share some of the responsibility for the money that had been lost.

The bank said the returns Mr S was being offered were too good to be true. He hadn't taken any steps to check the investment was legitimate or questioned why he was paying his investment funds to a personal account. The bank refunded Mr S half of the value of the last two payments he'd sent and it paid him a further £50 for the time it had taken to review his claim.

Our Investigator looked into everything. Under the terms of the CRM code, she thought Halifax should also refund 50% of the first two payments (in addition to the refund already offered by Halifax for the third and fourth payments).

She agreed though that Mr S should share some responsibility for the loss that had resulted. She thought a fairer reflection of the distress caused to Mr S would be for Halifax to pay an additional payment of £100 on top of the £50 Halifax had already paid.

Mr S didn't agree. He pointed out that other people had been refunded in full. He'd been told about the investment by a long-standing friend, and he'd taken that on trust.

Halifax also didn't agree with the Investigator. It said that it had made the original offer to partly refund Mr S before it had known there was an ongoing Police investigation into the trader. It said it wasn't established that the trader had been operating a scam or what Mr S's losses were. Halifax said we should wait for an outcome to the Police investigation to get that information.

In light of this disagreement, I've been asked to review everything afresh and reach a final decision on the matter.

### **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.

In deciding what's fair and reasonable in all the circumstances of a complaint, I'm required to take into account relevant: law and regulations; regulators' rules, guidance and standards; codes of practice; and, where appropriate, what I consider to be good industry practice at the time.

In broad terms, the starting position at law is that a firm is expected to process payments and withdrawals that a customer authorises, in accordance with the Payment Services Regulations and the terms and conditions of the customer's account. These were 'authorised payments' even though Mr S now believes he was the victim of a scam - Mr S made the payments himself. So, under the Payment Services Regulations 2017, and the terms and

conditions of his account, Mr S is presumed liable for the loss in the first instance.

However, where the consumer made the payments as a consequence of the actions of a fraudster as part of an APP Scam, the CRM Code can provide additional protections.

Halifax initially accepted that this was an APP scam. It said it would refund Mr S in part. But it now argues that this hasn't been shown that Mr S's money was lost to a scam. That would mean that no protection would be available to Mr S under the CRM Code.

### *Does the CRM Code apply to Mr S's payments?*

I've considered Halifax's point that there may be an ongoing police investigation into the trader. Halifax explains that it now wishes to rely on a provision in the CRM Code<sup>1</sup> permitting it to delay reaching a reimbursement decision in such circumstances.

That provision can allow a firm to delay reaching a CRM Code decision about a claim. But I don't consider that provision has any reasonable application where a firm has *already made* that decision – simply put, a firm cannot delay reaching a decision which it has already reached. Halifax had already investigated Mr S's claim and given an answer.

While the bank didn't specifically reference the CRM Code in its answer to Mr S's claim, it accepted this as an APP Scam which it agreed to partially reimburse. The claim was one that fell within the scope of the CRM Code, and Halifax did not dispute this at that point (it has only done so subsequently).

In any event, I'm not persuaded that this provision (or the other linked points raised by Halifax) have the effect of meaning it would be premature for me to determine Mr S's complaint. Even if I was to accept that Halifax had not considered the claim under the CRM Code previously (and on the contrary I consider that did happen) then the relevant provision requires that the outcome of the ongoing investigation might reasonably inform the firm's decision. I don't find that second limb of the provision would be engaged in this case either.

Specifically, I don't find that the outcome of any ongoing investigation into the trader will have a material effect on the CRM Code decision Halifax was required to make at the time. The CRM Code does not make criminal prosecution a necessary requirement in determining if something is an APP scam. A balance of probabilities finding is sufficient. There is no need to await criminal prosecution to establish that what occurred was an APP Scam covered by the code.

Furthermore, in a complex case of alleged fraud, a police investigation and charging decision can easily take several years. And it may not happen at all, for a variety of reasons which may bear no relation to the question of this being an APP Scam. This service was set up to resolve complaints quickly and informally. It wouldn't be in line with that remit for me to cause further delay where I consider I can fairly and reasonably determine the complaint in front of me now. Based on the evidence I have seen about this trading scheme on this (and other complaints concerning the same trader) I'm satisfied I am in a position to reach such a finding.

In Mr S's case, I'm being asked to decide if Halifax, under the terms of the voluntary CRM Code, is liable to refund him because he was the victim of an APP Scam. I am doing so applying what I consider to be the balance of probabilities based on the available evidence.

---

<sup>1</sup> "If a case is subject to investigation by a statutory body and the outcome might reasonably inform the Firm's decision, the Firm may wait for the outcome of the investigation before making a decision."  
[CRM Code - R3(1)(c)]

I find the evidence is persuasive that Mr S's funds were lost to an APP Scam covered by the CRM Code. Furthermore, I'm persuaded that the amount Mr S has lost to this APP Scam can be determined, again by the application of the balance of probabilities.

Part of the information I have reviewed in making this finding has been provided by the bank that Mr S paid the funds to. This information was shared in confidence<sup>2</sup> and I will not detail it here. In summary though as it relates to this complaint, no legitimate trading activity took place using the funds Mr S paid. The evidence from that bank is consistent with the operation of a so-called Ponzi scheme – whereby early investors receive returns which are paid from later investments.

Under the CRM Code, the definition of an APP Scam includes payments where *“The Customer transferred funds to another person for what they believed were legitimate purposes but which were in fact fraudulent.”*

On a balance of probabilities I find that Mr S sent his funds to the trader believing this was a legitimate investment, but that the trader's purpose in obtaining those funds was not to invest those funds but was instead fraudulent. Halifax has not provided any persuasive evidence that would contradict this finding.

I'm satisfied that this was more likely than not an APP Scam and that the CRM Code should apply. Again, while I appreciate a police investigation may reveal more detail, I'm of the opinion that it is not in question that this was a scam, or that Mr S suffered a financial loss through these payments. Here, the outcome of any such investigation isn't necessary for a reimbursement decision under the CRM Code.

*Does Halifax need to reimburse Mr S under the terms of the CRM Code?*

Under the terms of the CRM Code, where a bank identifies the risk of an APP scam for a payment instruction, it is required give an Effective Warning (a scam warning).

Halifax accepts that it should have identified that the final two payments were out of character for Mr S and that it could therefore have done more to protect him from the risk of an APP scam.

But having reviewed Mr S's payment history, I think Halifax should have identified an APP Scam risk at the point of the first payment. That payment was significantly larger than the typical payments made by Mr S. It was being made to a personal account and a payee Mr S hadn't paid before. While Mr S had once before made a similar sized payment (in the period of account history provided by Halifax) I don't think that meant this new £20,000 payment shouldn't have prompted concern that there was a risk of financial harm through fraud or scam.

Under the provisions of the CRM Code, I therefore find Halifax should have provided Mr S with an Effective Warning at the point he was making payment one.

Halifax explains that it is unable to demonstrate what warning would have been shown to Mr S. It has provided an example of what Mr S might have seen, assuming he would have said the payment was for an investment.

I agree that if Mr S had been asked for the payment purpose, he'd likely have said it was for

---

<sup>2</sup> The relevant rules can be found in the Dispute Resolution chapter (3) of the Regulator's Handbook of Rules and Guidance (DISP). At DISP 3.5.9R, the rules state that “the Ombudsman may: [...] (2) accept information in confidence (so that only an edited version, summary or description is disclosed to the other party) where he considers it appropriate”.

investment purposes. I say that because he gave the payment reference: "Contract FX", which doesn't indicate he had any intention to disguise the reason for the payment. Therefore, while Halifax cannot establish what was shown to Mr S (if anything) I think if a scam warning was given then it was most likely the example warning message Halifax has provided.

That being said, to be an Effective Warning, the CRM Code says the warning message must be impactful enough to positively affect customer decision making and reduce the likelihood of an APP Scam succeeding. I don't find Halifax's warning would have met that minimum requirement. The message didn't provide sufficient information to enable a customer to identify whether they were being asked to make the payment as part of a scam or provide the customer with steps they could take in order to protect themselves.

To summarise, under the CRM Code, Halifax needed to give an 'Effective Warning' at the point of payment one, but it did not do so.

I've seen nothing that would lead me to believe that had Halifax provided an Effective Warning, Mr S might have ignored the warning and proceeded regardless. On the contrary, I think the risk of the supposed investment being fake and a scam would likely have reinforced the doubts he already had and likely led to him deciding not to proceed (as he'd previously decided when the investment had been mentioned to him earlier). As a result, he'd likely not have made this or the subsequent payments.

The failure of Halifax to provide an Effective Warning at the point of payment one therefore had a material effect on the ultimate success of the scam Mr S fell victim to. That means I find that under the terms of the CRM Code, Halifax is required to refund, at least a proportion of each of the four payments Mr S made.

*Should Mr S share responsibility for the losses?*

The CRM Code says that where a firm can establish that a customer made an APP Scam payment without holding a reasonable basis for believing they were paying a legitimate payee for a genuine service, then it can choose not to fully refund them.

Here Mr S explains why he believed he was paying a legitimate trader for a genuine investment. He'd been recommended to the trader by a longstanding friend whom he trusted. This friend knew someone who'd said they'd made profits from the investment. While Mr S didn't receive any paperwork or brochures, he did later receive a contract.

There were some features here that I think would have provided some reassurance that this was genuine. And I take Mr S's point about the power of trusting his friend. However, there were also features that I think ought reasonably to have led Mr S to doubt what he was being offered by the trader.

He was being guaranteed he couldn't lose money from this investment, but the rate of return was exceptionally high. A rate of 10% a month compounded would mean the investor would supposedly be receiving three times their money back in less than a year and without any risk. That is simply too good to be true. I think Mr S knew this, and he acknowledges that when his friend first told him about the trader and the investment, he had doubts about it.

Mr S says he tried to carry out some checks into the investment (to carry out his due diligence) but he couldn't because there was nothing to look into further - there was no website or company to search for information about. Arguably, not being able to carry out any checks into who he was investing with should have been a red-flag in itself. Combined with returns that were too good to be true, this should have prompted significant doubts.

Mr S was putting a huge amount of trust someone he only knew indirectly. While Mr S's friend had told him about their own friend, in turn whose brother had supposedly profited from an investment with the same individual, I don't think that was much evidence to go on before sending a bank transfer of Mr S's life savings. Nor to make an investment of such a size by payment to a personal bank account. After all, his friend (or his friend's friend and her brother) might also have been deceived - as was the case here.

While I appreciate Mr S would never knowingly have paid money to something he thought wasn't a genuine investment, I think he did identify concerns here, and was right to, given the features of the supposed investment. Reasonably, I think he should have trusted those instincts and not invested at all.

That means I think Halifax is able to establish that Mr S made these payments without having held a reasonable basis for believing he was paying a legitimate financial trader for a genuine investment. Under the terms of the CRM Code Halifax does not need to refund Mr S in full. It should refund him 50% of the payments he made.

### *In summary*

The CRM Code applies to these payments and under the terms of the code, Halifax should have refunded Mr S half of what he lost.

I do not know exactly what Mr S would have done with the money he has not yet been reimbursed had Halifax refunded him when I think it should have. A small portion of the amount Halifax should now refund to Mr S represents funds borrowed from a family member. There is no simple way to accurately redress this situation. On balance, I think it would be fairest to add interest to the amount to be refunded at the rate of 8% simple per year to reflect the length of time Mr S has been deprived of these funds. That mirrors the rate Halifax applied when it initially agreed to partly refund Mr S. This calculation should apply from the point at which Halifax ought to have provided Mr S with a response to his scam claim under the CRM Code (the CRM Code requires a decision to be given within 15 days from the date of the claim).

Mr S has explained about the impact this has had on him. Of course, the bulk of that impact is down to the actions of those who defrauded him. But taking into account the time it took for Halifax to respond to Mr S's claim and the impact this had on him, I think it's fair that Halifax should pay a further £100 in respect of the additional distress and inconvenience caused by the bank's delays in handling his APP scam claim.

### **Putting things right**

To put matters right, Bank of Scotland plc trading as Halifax should (within 28 days of receiving confirmation that Mr S accepts my decision):

- Pay Mr S half of the total value of the payments he made to this scam, deducting any payments it has already refunded to him, and deducting any money that was otherwise recovered and returned to him;
- Add interest to the resulting amount at a rate of 8% simple calculated from 15 days after Halifax was first notified of Mr S's claim, until the date of settlement (Halifax can allow for any such interest it has already paid to Mr S); and,
- Pay an additional £100 in respect of the distress and inconvenience caused to Mr S by the time taken to deal with this matter.

**My final decision**

For the reasons given above, I uphold in part Mr S's complaint about Bank of Scotland plc trading as Halifax.

Under the rules of the Financial Ombudsman Service, I'm required to ask Mr S to accept or reject my decision before 10 April 2025.

Stephen Dickie  
**Ombudsman**