

The complaint

Mr and Mrs W have complained Bank of Scotland plc trading as Halifax won't refund several payments they say they made and lost to an investment scam.

Mr and Mrs W's representative referred the complaint to us, but for ease I will just refer to Mr and Mrs W throughout.

What happened

The background to this complaint is well known to all parties, so I won't repeat it in detail here. In summary, Mr and Mrs W fell victim to an investment scam after coming across the "opportunity" via messenger app groups. They say they read online articles and reviews as part of their due diligence prior to contacting the scammers. Once they did contact the scammers, they gained access to a sophisticated platform, downloaded screensharing software and were guided on how to use a cryptocurrency exchange to transfer funds to it. In total they sent more than £7,000, via three payments, in January 2022. They realised they had been scammed when they were told they needed to deposit further funds to make a withdrawal.

Halifax didn't reimburse Mr and Mrs W's lost funds and so they referred their complaint to us. Our Investigator looked into things but didn't recommend the complaint be upheld. They weren't persuaded, on balance, that Halifax could have prevented Mr and Mrs W from falling victim to the scam. They found that where Halifax did intervene, with human intervention, Mr and Mrs W were not entirely open and honest as to what they were doing with their funds. Mr and Mrs W disagreed.

As our Investigator couldn't resolve the matter informally, the case have been passed to me to issue 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.

I'm aware that I've summarised this complaint briefly, in less detail than has been provided, and in my own words. No discourtesy is intended by this. Instead, I've focussed on what I think is the heart of the matter here. If there's something I've not mentioned, it isn't because I've ignored it. I'm satisfied I don't need to comment on every individual point or argument to be able to reach what I think is the right outcome. Our rules allow me to do this. This simply reflects the informal nature of our service as a free alternative to the courts.

I don't doubt Mr and Mrs W have been victims of a scam here; they have lost a large sum of money and have my sympathy for this. However, just because a scam has occurred, it does not mean Mr and Mrs W are automatically entitled to recompense by Halifax. It would only be fair for me to tell Halifax to reimburse Mr and Mrs W for their loss (or a proportion of it) if: I thought Halifax reasonably ought to have prevented all (or some of) the payments Mr and Mrs W made, or hindered the recovery of the payments they made – whilst ultimately being

satisfied that such an outcome was fair and reasonable for me to reach.

I have kept in mind that Mr and Mrs W made the payments themselves and the starting position is that Halifax should follow its customers' instructions. So, under the Payment Services Regulations 2017 (PSR 2017) they are presumed liable for the loss in the first instance. I appreciate that Mr and Mrs W did not intend for their money to ultimately go to fraudsters, but they did authorise these payments to take place. However, there are some situations when a bank should have had a closer look at the wider circumstances surrounding a transaction before allowing it to be made.

Considering the 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 - Halifax should fairly and reasonably:

- Have been monitoring accounts and any payments made or received to counter various risks, including anti-money laundering, countering the financing of terrorism, and preventing fraud and scams.
- Have had 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 payment service providers 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 decline to make a payment altogether, to help protect customers from the possibility of financial harm from fraud.

So, I've thought about whether the transactions should have highlighted to Halifax that Mr and Mrs W might be at a heightened risk of financial harm due to fraud or a scam. Whilst doing so, I have kept in mind these transactions occurred in January 2022 – where awareness of cryptocurrency investment scams was not to the same level as it is now. Having carefully considered this, I've decided to not uphold Mr and Mrs W's complaint. I know this will come as a disappointment to them and so I will explain below why I've reached the decision I have.

Halifax did not allow the payments Mr and Mrs W were first attempting to make until they had first spoken with them. After Mr W confirmed some general details with Halifax the block was removed. However, when they then attempted to make their transaction to the cryptocurrency exchange, it was again blocked. Mr W spoke with Halifax again and was asked some further questions about the actions being taken.

However, although Halifax *could* have probed more, Mr W was not forthcoming with the details that would have allowed Halifax an opportunity to uncover he and Mrs W were being scammed from what it did ask. Having listened to the call I can see how the answers Mr W provided gave Halifax the impression he was only investing in the cryptocurrency exchange. For example, when he was asked how long he had been investing with the cryptocurrency exchange, Mr W did not correct Halifax that this was just being used as an intermediary tool after having received guidance via screen sharing as to what to do. Instead, Mr W confirmed he had set his account up with the cryptocurrency exchange around a month ago, this was a fairly new investment, it was being transferred into his own account, he wasn't transferring it to anyone else, it was his own decision to do so, that he was sensible enough not to be sending his funds to another country (which does highlight some awareness to scams), and that no-one had been in contact with him via phone or social media to transfer money to

another account. When asked how he came to find out about this company, Mr W said he came across it through months of research – rather than sharing that another entity was involved at any point. He also highlighted his previous investment experience with penny stocks, which tends to be another volatile market and suggested he had the level of risk awareness necessary for cryptocurrency. Had Mr W shared where he was sending the funds after the cryptocurrency exchange, as this was a known scam, Halifax would have been able to highlight this was a scam.

Mr and Mrs W believe Halifax should have probed further, but I don't agree. Halifax's interventions must not amount to interrogations. As per Mr and Mrs W's testimony this was a sophisticated scam, with a personalised access to a fake platform.

Overall, this level of caution from Halifax was reasonable considering the amount of money Mr and Mrs W were attempting to send to cryptocurrency. However, just because payments were being made to cryptocurrency, especially at the time of these payments, without there being any wider red flags, it would not automatically have caused Halifax to establish they were being scammed – or that there were additional details Mr W was not sharing. Halifax did make Mr W aware of the risks of investing in cryptocurrency. But ultimately buying cryptocurrency is a legitimate activity and it wasn't / isn't uncommon for retail investors to choose to invest funds in it. The exchange in question is also a legitimate one.

Consequently, I do not consider that Halifax needed to take any further action at this time based upon what Mr W had shared. Nor would I have expected it to have intervened further in these circumstances.

I am sorry to hear of the losses Mr and Mrs W have incurred from this cruel scam. I do not doubt they entered into this investment believing it to be a genuine opportunity. However, I cannot fairly say in this instance that Halifax should be held liable for their losses.

Recovery

I have gone on to consider if Halifax took reasonable steps to try and recover the funds. As these payments were made by debit card the option available is a chargeback. However, Mr and Mrs W made the transfer to their own account at the cryptocurrency exchange and ultimately did receive the expected service. Therefore a chargeback would not be successful and so I won't be asking Halifax to do anything further.

The Contingent Reimbursement Model Code

Although Halifax have signed up to the Contingent Reimbursement Model Code, the payments Mr and Mrs W made from their account aren't covered by the Code because they used their card. Although, even if the payments were made via a transfer that would also not have been covered because it would have been to an account in their own name, not another person. I cannot fairly and reasonably say that Halifax should have to refund payments under the Code when it doesn't apply here.

So, in light of all of the above findings, there's no fair and reasonable basis under which I can ask Halifax to reimburse Mr and Mrs W's loss.

My final decision

My final decision is I do not uphold this complaint against Bank of Scotland plc trading as Halifax.

Under the rules of the Financial Ombudsman Service, I'm required to ask Mr W and Mrs W

to accept or reject my decision before 12 December 2025.

Lawrence Keath
Ombudsman