DRN-5412972

The complaint and background

Mr N complains Bank of Scotland plc trading as Halifax won't refund the money he lost when he fell victim to a cryptocurrency investment scam.

Our investigator didn't uphold the complaint. She concluded Halifax wasn't liable for Mr N's loss as she didn't think it had cause to suspect he was falling victim to a scam, and to take further action to protect him, at the time.

Mr N's representative disagreed. It said while the size of the individual payments weren't out of character, Halifax should have been concerned about Mr N paying a new payee who was a cryptocurrency provider. It also said the second scam payment was a significant increase in value compared to the first scam payment sent the previous day.

Following this appeal, I issued my provisional decision on this complaint. I agreed with the investigator that the payments to the cryptocurrency wallet didn't look suspicious. However, I found there had been further attempts to top up Mr N's cryptocurrency wallet (to fund payments to the scam) – which I considered likely to have been initiated from this account. But in the absence of further context about why the top-ups failed, I still wasn't persuaded Halifax ought to have prevented this scam.

I invited both parties to submit any further comments or evidence. Halifax has confirmed it agrees with my decision and has nothing further to add. Mr N's representative has rejected the decision without submitting any further points to consider.

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 the absence of any further comments or evidence, I see no reason to depart from my provisional findings. For the reasons explained below, I've therefore decided not to uphold this complaint.

It isn't in dispute that Mr N authorised the payments in question. He is therefore presumed liable for the loss in the first instance. However, at the time of the payments, Halifax should have been on the look-out for fraud and made additional checks before processing payments in some circumstances. That is taking into account longstanding regulatory expectations and requirements, and what I consider to have been good industry practice at the time.

I have reviewed Mr N's account and the payments he made to the scam. Having considered when they were made, their value and who they were paid to, I'm not persuaded that Halifax ought to have found any of the payments suspicious, such that it ought to have made enquiries of Mr N before processing them.

I accept the payments were being used to top up Mr N's cryptocurrency wallet. However, as the payments Mr N made were faster payments, I'm not persuaded that would have been clear to Halifax based on the payment information. The funds were sent to an authorised Electronic Money Institute which provides a range of payment services. While that includes providing banking services in relation to cryptocurrency wallets, it also provides other types of accounts.

That said, Mr N's cryptocurrency wallet records also show several failed attempts to top up the wallet by card in between the successful transfers. Halifax says its records don't capture whether or not these were attempted using Mr N's Halifax debit card. But Mr N says he used his Halifax account to (attempt to) make these payments. He doesn't think Halifax stopped any payments, but suggests the top-ups may not have gone through due to an error by the wallet provider.

On balance, I consider it likely the top-ups were attempted using Mr N's Halifax debit card. That matches what Mr N recalls. It also looks to me as though he paid money into his Halifax account around the time of one of the attempted card payments in order to ensure he had enough in his account to fund this (before proceeding to transfer a smaller amount when it didn't go through).

I've considered whether that changes things. It suggests Halifax may have been able to see Mr N was attempting to pay a merchant providing exclusively cryptocurrency-related services. Furthermore, the size of the largest attempted card payment (around £4,500) was higher than the largest transfer (around £2,500, sent later that day after the card top-up failed). That would affect how risky the account activity looked.

However, even if Halifax could see the details of these payment attempts, that doesn't automatically mean it should have treated them as suspicious in the absence of other concerning factors. Looking at Mr N's account history, I can see he had still made other payments for a similar amount in the year or so leading up to the scam, and had also made a higher payment (for £5,000).

There is also a lack of clarity around why the top up attempts failed. This could have occurred for a number of reasons. For example it's possible Mr N entered some of the payment details wrong. Or, as he has suggested, there could have been an error by the merchant which prevented it from processing card top-ups at the time.

I think that makes it harder for me to conclude it's likely these failed top ups should have prompted further enquiries by Halifax. It leaves open the possibility Halifax wouldn't have been aware Mr N was attempting the card payments.

I've carefully thought about what Halifax should have known at the time. On balance, I'm not persuaded it ought to have been so concerned about the account activity such that it should have known to make further enquiries. I consider it reasonable that Halifax simply processed the payments in line with the authorised instructions it received from Mr N.

Overall, while Mr N has undoubtedly fallen victim to a cruel scam, I don't find there were any failings on Halifax's part that would lead me to uphold the complaint.

My final decision

For the reasons given above, my final decision is that I do not uphold this complaint.

Rachel Loughlin
Ombudsman