DRN-4153486

The complaint

Mr D complains that Bank of Scotland plc trading as Halifax did not refund a series of payments he lost to a scam.

What happened

Mr D was approached by his brother who had joined a cryptocurrency investment scheme into Ethereum mining via a business he felt was legitimate. His brother, along with other friends, had been shown returns on their investments and had been involved in the scheme for many months. Because of this, Mr D was convinced to join. Mr D intended to transfer funds to a cryptocurrency account in his own name, purchase USDT and then transfer the funds on to the scheme.

He made an initial payment of £10,000 to the cryptocurrency account in his own name. This was flagged by Halifax as requiring additional checks and there was a telephone conversation between them and Mr D. They asked Mr D a few questions and gave a general scam warning before releasing the funds. Mr D went on to make a £65 payment which he says was a fee and a £4,000 payment the following day, neither of which were flagged by Halifax.

A few weeks later, Mr D started to become suspicious, but the scammer showed evidence of his returns. However, when Mr D attempted to make a withdrawal a few weeks after that, he received automatic replies asking him to pay tax to withdraw the funds. After numerous automatic replies he realised that it was a scam and contacted Halifax a few days later.

Halifax issued a final response to Mr D's claim declining to refund him. They said that as the payments went to an account in Mr D's own name, they could not recover the funds and the Contingent Reimbursement Model (CRM) did not apply to his case. They said that Mr D was not honest with them when the £10,000 payment was flagged. They said they asked him if anyone had advised him to make the payment and he said no, even though his brother had advised him to. And that he was only purchasing a currency called USDT, when he was in fact investing in Ethereum mining via a third party.

Mr D referred the complaint to our service and our Investigator looked into it. They agreed the complaint was not covered by the CRM code and that Halifax acted reasonably when they declined to uphold it. And that even if Mr D had been questioned further by Halifax, they didn't think the scam would have been prevented as he trusted his brother's advice.

Mr D disagreed with this and felt Halifax could have done more to advise him of the risks of it being a scam.

As an informal agreement could not be reached, the complaint has been passed to me for 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.

Having done so, I don't direct Halifax to refund the transactions in question and I do not uphold this complaint; I'll explain why in more detail.

Firstly, I agree that this complaint is not covered by the CRM code as the funds were sent between two accounts in Mr D's name. Because of this, Halifax only had a responsibility to monitor Mr D's account for unusual transactions.

To explain in more detail, broadly speaking, the starting position in law is that an account provider is expected to process payments and withdrawals that a customer authorises it to make, in accordance with the terms and conditions of the account. And a customer will then be responsible for the transactions that they have authorised.

It's not in dispute here that Mr D authorised the three payments totalling £14,065. So, while I recognise that Mr D didn't intend the money to then go to a scammer, the starting position in law is that Halifax was obliged to follow Mr D's instruction and process the payments. Because of this, Mr D is not automatically entitled to a refund.

The regulatory landscape, along with good industry practice, also sets out a requirement for account providers to protect their customers from fraud and financial harm. And this includes monitoring accounts to look out for activity that might suggest a customer was at risk of financial harm, intervening in unusual or out of character transactions and trying to prevent customers falling victims to scams. So, I've also thought about whether Halifax did enough to try to keep Mr D's account safe.

As mentioned previously, Halifax did flag the initial payment of £10,000 as suspicious and telephoned Mr D prior to processing it. Having looked at Mr D's regular account history, I think it was reasonable that this payment was flagged as it was of a relatively high value and higher than the usual payments on the account.

I've gone on to look at the phone call between Halifax and Mr D, which I have been provided a transcript of. In this, I can see that Mr D was asked some relevant questions such as, was he intending to trade and were the payments for an investment, which Mr D answered no to. While this particular payment was intended to go to his own wallet to purchase USDT, it was then going to a 'group fund' to invest in a company specialising in Ethereum mining. So, I don't think that Mr D answered as clearly and honestly as he could have done in this situation.

However, I do think that Halifax could have probed a little further as they only asked surface level questions. Especially as Mr D had recently received a loan from a friend to help fund the payment. And I think the warning they provided was very general and not specific to cryptocurrency scams. Having said this, I don't think it would have made a difference if they had provided a more specific warning or probed further. I'll explain why.

Mr D had been informed of the 'investment' by his brother who had been involved in the scheme (as a victim) for some time prior to that. Mr D has explained that he was convinced by the scam because he had spoken with individuals, such as his brother and friends, who had been involved in the scheme for some time and he was shown evidence suggesting payments were being made and reinvestments were successful. So, he felt it was a legitimate business. Considering all of this, I don't think it's likely that further questions by Halifax or a more specific scam warning would have been enough to break the spell of the scam, as individuals that Mr D trusted also felt it was legitimate.

The following two payments of £65 and £4,000 were not particularly unusual or out of character considering Mr D’s general account activity. I can see that Mr D had made other payments of a similar value and the higher payment of £4,000 was not so significant that I think its value alone warranted further checks. So, I don’t think Halifax made an error when it did not flag these as unusual or suspicious.

As has already been explained to Mr D, it was not possible for Halifax to recover the funds, as they went to an account in his own name and by the time Mr D made Halifax aware – there were no funds remaining left to recover.

In summary, I think that Halifax correctly flagged the payment that was unusual when compared to Mr D’s normal account activity and I don’t think it made an error when it didn’t flag the later two. While I do think that Halifax could have provided more focused cryptocurrency scam warnings, I don’t think these would have been enough to reveal the scam due to the way in which Mr D was introduced to it. And I don’t think Halifax could have reasonably recovered the funds once they were aware of the scam. So, I don’t think Halifax needs to take any further action in relation to this complaint.

My final decision

I do not uphold Mr D’s complaint against Bank of Scotland plc trading as Halifax.

Under the rules of the Financial Ombudsman Service, I’m required to ask Mr D to accept or reject my decision before 10 October 2023.

Rebecca Norris
Ombudsman