

The complaint

Mr L complains that Bank of Scotland plc, trading as Halifax, did not refund the money he lost as part of a scam.

What happened

Mr L was approached on a social media platform by an 'advisor' who offered to help him invest in cryptocurrency. Mr L felt he could trust the advisor as they had a large following as well as testimonials from satisfied customers on their page. Mr L initially invested £350 and was assured he would receive £3,500 the following day. However, he was then told he needed to pay additional fees for the funds to be released, which he did so over the next two days. He chased the advisor and the other individual he had spoken to but received no response. He says that he realised it was a scam at that point as he no longer had access to his funds and though he had been told his investment had grown to £7,000, he was not given access to this.

Mr L then made further payments in June over a few days, however he has not provided us with a reason as to why these further payments were made and he cannot locate the correspondence between himself and the scammer in relation to these. Mr L lost just over £5,000 to the scam.

Mr L contacted Halifax on 31 August 2022 to raise a claim for the transactions he felt were fraudulent.

Halifax issued a final response letter on 20 December 2022 in which it explained that as Mr L had authorised the transactions, they would not look to refund him. Mr L referred the complaint to our service and our Investigator looked into it. They explained that as the payments had been made with a debit card, they could not be considered under the contingent reimbursement model (CRM) code. Overall, they did not feel the transactions were of a high enough value to warrant additional checks by Halifax and they also had no basis for a chargeback request. In addition, they felt that Mr L should have asked more questions before proceeding with the payments.

Mr L's representative disagreed with the outcome. They felt that the payments were an anomaly and did not represent Mr L's usual spending patterns. As Mr L had no prior dealings with cryptocurrency trading, they said he was more vulnerable to this type of 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.

I have no reason to doubt that the March payments were made as part of a scam, and Mr L has provided his communications with the scammer to evidence this. However, it is unclear

to me if the June payments were part of the same scam as no evidence has been provided to me about them. Mr L has been able to provide older correspondence about the March payments but none for the June ones. And he has said that he became suspicious when he could not contact the advisor after the March payments. It is therefore unclear why he went on to make further payments for cryptocurrency in June. However, for completeness, I have gone on to consider all of the payments raised and whether Halifax should reasonably have done more in the circumstances.

In line with the Payment Services Regulations 2017 (PSRs), Mr L isn't liable for payments he didn't authorise, unless he failed with gross negligence or intent to comply with the terms of the account or keep his personalised security details safe. Accordingly, I've considered whether Mr L authorised the payments in question here.

Having done so, I can see that it is not in dispute that Mr L authorised the payments to a cryptocurrency account, using his debit card. So, while I recognise that Mr L thought he was investing his funds and would see returns, this doesn't change the fact that he authorised them and is therefore presumed liable for the loss in the first instance.

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 L's account safe.

In my opinion, the payments in question just weren't sufficiently unusual, uncharacteristic or suspicious to reasonably say Halifax should not have processed them without first getting in touch with Mr L to ensure they were legitimate and not related to a scam. The values of the transactions ranged from around £25 to just over £1,000 which are not particularly high. And when compared with Mr L's normal account activity, they do not stand out as unusual, as there were other payments for similar amounts being made on the account.

The cryptocurrency exchange that Mr L made the payments to is a legitimate company and it should be noted that not all payments made for cryptocurrency are a result of a scam. In this case, I don't think where the payments were headed ought to have automatically triggered Halifax's attention.

Considering all of this, as Halifax didn't interact with Mr L prior to the payments being made, and I think the payments weren't so unusual that they ought to have contacted him prior to them being processed, I don't think they missed an opportunity to prevent the payments before they were sent.

Mr L made Halifax aware of the scam on 31 August 2022, over five months after the initial payments were made. As the payments were made by debit card, the only recourse for potential recovery would be through the chargeback scheme. The chargeback scheme is voluntary and there is no guarantee of a refund when it is used. It is a process by which disputes can be resolved through card issuers, such as Halifax, and the merchant. So, I've considered whether Halifax should have raised a chargeback claim for Mr L.

Halifax has stated that as the payments were made to a legitimate company to purchase cryptocurrency, they had no grounds for a chargeback claim, and I agree with this. As it was a legitimate business that provided the services, i.e., the purchase of cryptocurrency, as intended, there would be no reasonable grounds for a chargeback to be raised.

In any event, the March payments were made outside of the 120-day time limit for a

chargeback as Mr L did not raise the complaint until 31 August. As I explained earlier, it is unclear to me if the June payments were part of the scam.

As explained above, I do not think that Halifax should have flagged the payments as unusual or suspicious, and I think Halifax reasonably concluded there were no grounds for a chargeback claim. So, I do not direct Halifax the refund the transactions in question.

My final decision

I do not uphold Mr L's complaint against Bank of Scotland plc, trading as Halifax. I

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

Rebecca Norris
Ombudsman