DRN-5670514

The complaint

Mr H complains that Starling Bank ("Starling"), have failed to refund money that he lost as part of a scam.

What happened

Mr H met a person online. After a few weeks this person who I will call C persuaded Mr H to invest in a scam crypto trading company. These transactions were over 15 transfers to a crypto exchange and what appears to be two peer to peer crypto transactions. These transactions took place between September 2024 and January 2025 and totalled over £19,000.

Initially the transactions were for investing and trading, but towards the end, they were to pay fees to enable Mr H to keep and withdraw his profits.

Mr H eventually realised that C was a scammer when he remained unable to access the profits that he thought he had made.

One of our investigators looked into this matter and he did not think that Starling could have uncovered or prevented the scam.

Mr H did not agree with these conclusions and so his complaint has 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.

Having done so, I agree with the conclusions reached by the investigator for the following reasons.

In broad terms, the starting position is that Starling is expected to process payments and withdrawals that a customer authorises it to make, in accordance with the Payment Services Regulations and the terms and conditions of the customer's account.

But, taking into account relevant law, regulators' rules and guidance, relevant codes of practice and what I consider to have been good industry practice at the time, I consider it fair and reasonable that Starling should:

- have been monitoring accounts and any payments made or received to counter various risks, including 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 firms are generally more familiar with than the average customer;

- in some circumstances, irrespective of the payment channel used, have taken additional steps, or made additional checks, or provided additional warnings, before processing a payment

- have been mindful of – among other things – common scam scenarios, how the fraudulent practices are evolving (including for example the common use of multi-stage fraud by scammers, including the use of payments to cryptocurrency accounts as a step to defraud consumers) and the different risks these can present to consumers, when deciding whether to intervene.

In this instance, the initial payments were small and the pattern of payments did not indicate that Mr H was likely being scammed. That said, I think that the payment of £5,000 that Mr H made on 7 January 2025 should have prompted an intervention from Starling due to its size. I think that an appropriate intervention would have been for Starling to ask questions about the payment that Mr H was making and provide an appropriate warning based on the answers Mr H provided.

But I don't think that this would have stopped the scam. I say this because I can see that the crypto exchange did warn him around this time that what he was doing was likely a scam and it even stopped a payment. Mr H then was instructed by the scammer to appeal the payment being stopped and told him what to do to get the payment released. I can also see that during an attempted transaction from a different current account that Mr H held with a different provider, when it asked about reasons for the payment Mr H asked the scammer what to say, and it appears that he provided the answers that the scammer told him to put in. This suggests that, had Starling asked questions, Mr H would likely have asked the scammer what to say to allow the payment to go through. I think this would likely have made any warning not relate to the scam and would likely have meant that the payment would not have been stopped either.

It is clear that by this point Mr H was heavily under the spell of the scammer and that he believed he was in a serious relationship with the scammer. Given this, I think that had Starling intervened, the scammer would have been able to persuade him to provide answers that would allow the payments to go through. Also, if Starling had managed to provide some form of crypto scam warning, I think that the scammer would have been able to persuade him to make the payments regardless of the intervention. Finally, even if Starling had stopped the payments entirely, given the relationship between him and the scammer, I think Mr H would have found a different way to make the payments.

So, taking everything into consideration, I do not think that Starling could have uncovered and prevented the scam even if it had intervened.

I've also thought about whether Starling did enough to attempt to recover the money Mr H lost. In this instance the transfers would not be covered by the Authorised Push Payment (APP) scheme or the Contingent Reimbursement Model, as the funds were being sent to an account in Mr H's own name. In relation to the peer-to-peer crypto payments, they are not covered by either scheme. I also don't believe there were any other ways for Starling to recover the funds.

I appreciate this will likely come as a disappointment to Mr H, and I'm sorry to hear he has been the victim of a cruel scam. However, I'm not persuaded that Starling can fairly or reasonably be held liable for his losses in these circumstances.

My final decision

My final decision is that do not uphold this complaint.

Under the rules of the Financial Ombudsman Service, I'm required to ask Mr H to accept or reject my decision before 5 December 2025.

Charlie Newton
Ombudsman