

## **Complaint**

Mrs B is unhappy that Starling Bank Limited didn't agree to refund her after she fell victim to a scam.

## **Background**

In late-2023, Mrs B was contacted in connection with a job opportunity. The role was flexible in terms of the hours expected and could be completed remotely. She was told that she would be asked to complete tasks on a platform maintained by the employer. The premise was that these tasks would assist clients of the employer with "app optimisation." Unfortunately, this wasn't a legitimate job opportunity. Mrs B had been targeted by a fraudster.

She was told that she would earn commission for each task completed. However, her account on the company's platform needed to be funded. She was asked to make payments to the company platform to enable her to earn and access the commission payments she thought she'd be entitled to. She made those payments in the expectation that she'd earn back significantly more in terms of commission.

She used her Starling account to make around ten payments. The total value of those payments was a little over £18,000. These were payments to private individuals or companies, but they appear to have been made to finance peer-to-peer cryptocurrency purchases. In other words, she was purchasing existing cryptocurrency that was owned by someone else. Once that cryptocurrency came into her possession she transferred it into the control of the fraudsters.

Once she realised she'd fallen victim to a scam, she notified Starling. It didn't agree to refund her losses. Mrs B wasn't happy with that response and so she referred her complaint to this service. It was looked at by an Investigator who didn't uphold it. Mrs B disagreed with the Investigator's opinion and so the complaint has been passed to me to consider and come to a final decision.

## **Findings**

I've considered all the available evidence and arguments to decide what's fair and reasonable in the circumstances of this complaint.

In broad terms, the starting position at law is that a firm is expected to process payments and withdrawals that a customer authorises, in accordance with the Payment Services Regulations (in this case, the 2017 regulations) and the terms and conditions of the customer's account. It's common ground that Mrs B authorised these payments and so she is presumed liable at first instance.

These payments aren't covered by the Lending Standards Board's Contingent Reimbursement Model Code ("CRM Code") because they don't meet its definition of an authorised push payment (APP) scam. For the purposes of this case, these payments need to be ones where *"the Customer transferred funds to another person for what they believed*

*were legitimate purposes but which were in fact fraudulent.*” These payments were peer-to-peer cryptocurrency purchases. That meant Mrs B entered into a legitimate agreement to purchase cryptocurrency from a genuine seller who likely had no connection to the scam. The purpose for which that payment was made was legitimate even if she ultimately ended up transferring that cryptocurrency into the control of the fraudsters.

Nonetheless, good industry practice required that Starling be on the lookout for account activity or payments that were unusual or out of character to the extent that they might indicate a fraud risk. On spotting such a payment, I'd expect it to take steps to protect their customer. That might be as simple as providing a written warning as part of the payment process or it might extend to making contact with the customer to establish the circumstances surrounding the payment.

We now know with the benefit of hindsight that Mrs B was falling victim to a scam. The question I have to consider is whether that risk ought to have been apparent to Starling given the information that was available to it. I've considered that question carefully and I'm not persuaded it could reasonably have been expected to identify the fraud risk here. The payments weren't large enough that I'd have expected the bank to have concerns, unless there were other risk factors present. Mrs B was purchasing cryptocurrency and Starling should've been aware that payments connected to cryptocurrency have an associated fraud risk. However, as these were 'peer-to-peer' purchases, it wouldn't have known that this was what Mrs B was paying for.

I can see that she was asked to provide additional information about the purpose for which she was making these payments. Unfortunately, the answers she gave weren't accurate. She told Starling either that she was paying a bill or that she was transferring funds to friends/family. That put Starling in a much more difficult position when it came to weighing up whether there was a fraud risk here.

I do appreciate what Mrs B has said about why she answered its questions in the way she did. She says that she was following the instructions of her supervisor who told her what she needed to do to make sure the payments weren't held up by the bank. However, the consequence of her answering the bank's questions in the way she did was that it had no realistic chance of spotting that she was at risk of financial harm due to fraud.

For the sake of completeness, I've also looked at whether Starling did everything it could in respect of recovering Mrs B's money. However, given that these were peer-to-peer cryptocurrency purchases made from people that weren't connected to the scam, it couldn't have done anything to recover money from those recipients.

I don't say any of this to downplay or diminish the fact that Mrs B has fallen victim to a cruel and cynical scam. I have a great deal of sympathy for her and the position she's found herself in. Nonetheless, my role is to look at the actions and inactions of the bank and I'm satisfied it didn't do anything wrong here.

### **Final decision**

For the reasons I've explained above, I don't uphold this complaint.

Under the rules of the Financial Ombudsman Service, I'm required to ask Mrs B to accept or reject my decision before 25 July 2025.

James Kimmitt  
**Ombudsman**

