

## The complaint

Mrs T complains that Starling Bank Limited ('Starling') won't reimburse the funds she lost when she fell victim to a scam.

## What happened

Mrs T says that she was looking for part-time work to supplement her income, as her mother was ill and she wanted to help out. She provided some details to a company I'll call C and received a message from someone from the company. The role involved reviewing products and receiving commission and Mrs T was required to deposit funds so that she could complete tasks. Mrs T didn't know at the time, but the job was fake, and she was dealing with scammers.

I have set out in the table below the transactions Mrs T made on the instructions of the scammer. All were card payments to two digital remittance companies commonly used for international transfers.

Transaction	Date	Amount	Payee
1	26/07/24	£67.70	1
2	26/07/24	£43.06	1
3	27/07/24	£139.06	2
4	27/07/24	£493.44	2
5	27/07/24	£896	2
6	29/07/24	£375	2
7	31/07/24	£1,434.43	2
8	02/08/24	£1,318.38	2
9	05/08/24	£1,931.73	2
10	05/08/24	£267.45	2
11	07/08/24	£650	2

Mrs T says she realised she was the victim of a scam when she was unable to get in contact with anyone from C.

Mrs T's representative sent a letter of complaint to Starling in October 2024 and asked that it reimburse her in full under the Contingent Reimbursement Model Code (CRM Code) based on her vulnerability.

Starling asked for some additional information but didn't receive a reply. It issued a final response letter which said that on the limited information available, it didn't think it had done anything wrong.

Mrs T was unhappy with Starling's response and brought a complaint to this service.

### *Our investigation so far*

The investigator who considered this complaint didn't recommend that it be upheld. She said Starling acted reasonably in not taking any additional steps before processing the payments.

Through her representative, Mrs T didn't agree with the investigator's findings. In summary, she said:

- The transactions were uncharacteristic. Previous international payments were less frequent and of lower amounts. During the course of the scam, Mrs T made payments which totalled £7,564.16 in around ten days. Starling should have noticed the sudden increase in spending and contacted Mrs T. Had it done so, Mrs T said the scam would have been uncovered.
- Mrs T was vulnerable at the time and had Starling intervened it would have identified her vulnerability and prevented her loss.
- Starling failed to explore options other than chargeback to recover Mrs T's funds, such as contacting the international money remittance platforms involved.
- This service should require Starling to implement stronger fraud detection and intervention measures to prevent similar things happening in future.

### **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 deciding what's fair and reasonable, I am required to take into account relevant law and regulations; regulators' rules, guidance and standards; codes of practice and, where appropriate, what I consider to have been good industry practice at the time.

Mrs T's representative has said she should be reimbursed under the CRM Code. But this Code doesn't apply to card payments, or to payments made to an account in a customer's own name. In this case, Mrs T made card payments to two accounts in her name, so the CRM Code isn't relevant. I've considered Starling's broader obligations though.

In broad terms, the starting position at law is that a bank such as Starling is expected to process payments and withdrawals that a customer authorises it to make, in accordance with the Payment Services Regulations (in this case the 2017 regulations) and the terms and conditions of the customer's account.

I consider it fair and reasonable in July and August 2024 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;
- have acted to avoid causing foreseeable harm to customers, for example by maintaining adequate systems to detect and prevent scams and by ensuring all aspects of its products, including the contractual terms, enabled it to do so;
- 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 and the different risks these can present to consumers, when deciding whether to intervene.

I have considered Mrs T's statements from January 2024. Having done so, like the investigator, I'm not persuaded that the scam payments were so unusual and out of character that Starling ought reasonably to have intervened before processing them. I'll explain why.

Payees one and two are existing payees Mrs T had previously sent funds to and both are commonly used for international transfers. In March 2024 Mrs T made a card payment of £626.26 to payee two and in early July 2024 she made a payment of nearly £500 to payee one. Whilst the value of transactions seven, eight and nine were higher than previously, they weren't at a level where I'd have expected Starling to have concerns she was at heightened risk of being the victim of a scam. The three larger payments were each made a few days apart and there were no other unusual features that ought to have alerted Starling to the possibility of financial harm from fraud. There wasn't, for example, a pattern of increasing payments, and, although Mrs T's balance was low after some transactions, this wasn't unusual given the usual operation of the account.

A balance needs to be struck between Starling identifying potentially concerning payments, and responding appropriately to any concerns, and minimising disruption to legitimate payments. Overall, I don't think Starling acted unreasonably in processing the transactions Mrs T authorised without intervening.

I appreciate that Mrs T was going through a difficult time when she made the payments and am sorry to hear about her circumstances. As I have said above, the CRM Code doesn't apply in this case, so I am unable to consider its provisions in respect of vulnerability. And Starling was unaware of Mrs T's personal circumstances until after the scam was reported, so couldn't have put any additional measures in place when the payments were made. I agree that Mrs T's vulnerability would likely have been discussed if Starling had intervened when any of the payments were made, but, as I have explained above, I don't think Starling needed to do so.

For completeness, I've considered chargeback, which is a process that allows debit and credit card holders to reverse a transaction when there's a problem with the goods or services they have purchased. It is organised and run through the overarching card scheme but customers wishing to use the service must go through their card issuer (Starling in this case). The chargeback scheme is voluntary, and banks are not under any formal obligation to submit a chargeback claim. But this service's view is that it is good practice for a bank like Starling to make a chargeback claim where the right exists, timescales are met and there is a reasonable prospect of success.

In this case though, I consider that Starling acted reasonably in not raising a chargeback as there was no applicable chargeback reason, so no prospect of success. Mrs T made payments via a money remittance companies which provided the service expected – the money was transferred to the intended recipient. It wasn't the money transfer service which 'scammed' Mrs T out of the funds, but any chargeback would need to be raised against it.

As the payments were made by card to accounts in Mrs T's own name there was nothing Starling could have done to recover her funds.

Mrs T's representative has asked me to require Starling to improve its fraud detection systems. My role is to consider the individual circumstances of Mrs T's complaint and decide if Starling treated her fairly so this isn't something I can consider.

Overall, whilst I'm sorry to hear about this cruel scam and the impact it has had on Mrs T, I can't fairly require Starling to reimburse her loss.

**My final decision**

For the reasons stated, I do not uphold this complaint.

Under the rules of the Financial Ombudsman Service, I'm required to ask Mrs T to accept or reject my decision before 27 October 2025.

Jay Hadfield  
**Ombudsman**