

The complaint

Miss T is unhappy that Starling Bank Limited won't refund the remaining money she lost after she fell victim to an Authorised Push Payment (APP scam).

What happened

Both parties are aware of the circumstances of the complaint, so I won't repeat them all here.

But briefly, in July 2022, Miss T received a call from an individual purporting to be from Starling, telling her that her accounts were at risk. But unknown to Miss T at the time, the call was from a fraudster. Miss T has said, some time before she was called by the fraudster, she had clicked a link on her mobile phone and provided her card details, but realising this was a scam Mrs T had called Starling, at which time her card had been cancelled and replaced.

The fraudster suggested to Miss T that, to reassure herself that the call was genuine, she should verify the number she was being called from online. When Miss T did this, she says she could see it was a Starling number. The fraudsters told Miss T that she needed to move her money to a safe account in order to protect it, as fraudsters had access to all of her accounts.

Believing everything to be genuine, on 20 July 2022, Miss T was persuaded to move over £18,000 from a savings account she held with another banking provider into her Starling account. Following which, she made 37 payments in around 30 minutes to account details the fraudsters provided. In total, Miss T made payments totalling £19,240 from her Starling account to an account that was controlled by the fraudsters.

Miss T has said she was on the phone to the fraudster the whole time and was told she was making the payments for her own safety. Miss T has said that at the time, thinking her money was at risk, she felt rushed and was crying. She said she questioned the fraudster, but they comforted her and told her they were there to help. Miss T realised she'd been scammed when, after she'd moved all of her money, the line went dead.

Miss T contacted Starling to report that she had been the victim of a scam. Starling looked into Miss T's complaint and considered its obligations to provide her with a refund. Starling is a signatory of the Lending Standards Board Contingent Reimbursement Model (CRM) Code which requires firms to reimburse customers who have been the victims of APP scams like this in all but a limited number of circumstances. It says one or more of those exceptions applies in this case and that Miss T hadn't met the standards required of the Code.

In summary, in its final response letter, in November 2022, Starling recognised that, at the point Miss T made a payment at 16:58 on 20 July 2022 (for £680), it could have done more to protect her, so it accepted under the CRM code that it should share responsibility. With this in mind it agreed to refund 50% of Miss T's loss, from the point she had made the payment at 16:58 and it credited Miss T's account with £8,925.00.

Starling thought Miss T should also bear some responsibility for her loss. In summary this was because it didn't think she had a reasonable basis for belief that the person she was transacting with was legitimate. Starling added that Miss T was presented with warnings at the time she made the payments, however it said due to the value of the payments it did not present enhanced effective warnings.

Starling also tried to recover the money Miss T lost from the beneficiary accounts (the accounts to which the payments were sent). It was able to recover £2.97, which was returned to Miss T, but unfortunately no further funds remained to be recovered.

Starling recognised there was a delay in providing Miss T with a response to her fraud claim and because of this it compensated Miss T with £150.00.

Believing she should have been refunded in full Miss T referred her complaint to this service. One of our Investigator's looked into things and thought the complaint should be upheld. In summary, he didn't think Starling had established that Miss T didn't have a reasonable basis for belief, or that she had ignored an effective warning. He added that he thought there was enough going on, from the first transaction that Miss T made to the fraudsters, that ought to have prompted Starling to have intervened and he thought this intervention would have made a difference. It was our Investigator's view that Starling should refund Miss T the remaining money she lost, along with interest. Our Investigator also thought Starling should pay Miss T £250 for the trouble and upset caused.

Miss T agreed with our Investigator's view. Starling didn't agree, in summary it thought alarm bells should have rung with Miss T when she was asked to make 37 small transactions, rather than a bulk one.

As agreement couldn't be reached the complaint has been passed over 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.

In doing so, I'm required to take into account relevant: law and regulations; regulators' rules, guidance and standards; codes of practice; and, where appropriate, what I consider to be good industry practice at the time.

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 and the terms and conditions of the customer's account.

However, where the consumer made the payment because of the actions of a fraudster, it may sometimes be fair and reasonable for the bank to reimburse the consumer even though they authorised the payment. The CRM Code is of particular significance here. As I've mentioned, Starling is a signatory to that code, which requires its signatories to reimburse customers who are victims of scams like this one in all but a limited number of circumstances. Starling says that one or more of those exceptions are applicable in this case.

Did Miss T have a reasonable basis for belief?

I have thought carefully about whether Miss T had a reasonable basis for belief when making the payments and I'm persuaded that she did. I say that because;

- Shortly before the scam, Miss T had provided her bank card details after falling foul to a phishing scam. She reported this to Starling and new bank cards were issued. It seems the fraudsters were aware of this. So, when the fraudsters, when they called her, told Miss T that there was suspicious activity on her account, I think it is understandable and not unreasonable why she may have thought this was something her bank would want to discuss with her, as a matter of some urgency, if her accounts were at risk.
- The sophistication of the scam enabled the fraudster to spoof a bank's genuine telephone number which re-assured Miss T they were genuine. I'm also satisfied Miss T was unaware that phone numbers can be spoofed so that calls appear to come from a genuine source.
- Miss T also made attempts to verify the number she had been called on. Miss T has said the fraudster coached her through checking the number she was being called from online. Which I think reasonably gave her further assurances that she was genuinely talking to her bank.
- Miss T was being put under time pressure to move her money, in order to protect it, as is often the case for customers affected by this type of scam. I don't think Starling has given enough consideration to the fact the fraudster had created an environment where Miss T thought she had to act quickly to protect her accounts from an attack. With the benefit of hindsight and the removal of the pressured environment, it's easier to identify elements where Miss T may have had an opportunity to ask further questions. But the convincing nature of these scams can often have a negative effect on a person's thought process and make them take steps that, in the cold light of day, they might not otherwise take.

Overall, I'm not persuaded that Starling has done enough to establish that Miss T made these payments without a reasonable basis for believing that she was transacting with a legitimate employee of her bank.

Starling has acknowledged that it ought to have intervened sooner than it did. It has added that, while it did present Miss T with warnings at the time she made the payments, it didn't present enhanced effective warnings. In any event, I don't think the warnings Starling has said it *did* present could be considered as effective, under the CRM code. I say this because the warning wasn't specific to the scam that Miss T was falling victim to and doesn't give any detail about how these type of impersonation scams look and feel, such as fraudsters impersonating bank employees and having the ability to 'spoof' genuine telephone numbers. So, I don't think Starling has established that Miss T ignored an effective warning.

Considering everything, I'm persuaded that Starling should have reimbursed all the money Miss T lost from her Starling account under the CRM Code. I'm not satisfied that any of the permitted exceptions to reimbursement apply in the circumstances of this case.

Should Starling have done more to prevent the scam?

In addition, I think that Starling ought reasonably to have done more to prevent this scam.

Miss T transferred a large sum into her account to facilitate the payments to the fraudsters (over £18,000, which was not typical for her when compared to her account activity over recent months) and she then set up a new payee. When coupling this with what the bank

already knew, that Miss T had recently been the target of a phishing attack, I think Starling ought fairly and reasonably to have been on a heightened state of alert that she may have been at risk of financial harm.

Considering this, I think it's fair and reasonable to have expected Starling to have intervened and questioned Miss T at the point she was making the first payment to a new payee and for it to have asked Miss T some questions, before allowing the payments to be processed. Had it done so, I think the scam would've quickly unfolded and Miss T wouldn't have gone ahead with the first, or the subsequent payments.

The relevance of this finding is that Starling ought to have prevented the loss, rather than just reimbursed Miss T under the provisions of the CRM Code. It follows that Starling should pay Miss T interest from the date of loss, rather than the date it decided not to refund her under the CRM Code.

Service provided to Miss T

Starling has acknowledged that it could have dealt with Miss T's fraud claim better and it has given her £150 for delays, our Investigator thought this should be increased to £250.

Miss T has explained to this service the difficulties this fraud caused and the impact it had both financially and on her health. It is clear this was undoubtedly a very stressful and difficult time for Miss T, and while I recognise the fraudsters are the chief cause of the distress she's suffered, I agree that much of that could have been avoided had the bank acted sooner in both preventing the fraud and in reviewing her fraud claim in a more timely manner.

When thinking about this, I find that Starling should pay Miss T a further £100 for the distress and inconvenience caused, on top of the £150 it has already paid.

Putting things right

For the reasons explained above, I think it's fair and reasonable that Starling Bank Limited should now;

- Refund Miss T the remainder of the money she lost, less any money that it was able to recover.
- Pay interest on this amount, at the savings account rate from which the funds originated, from the date of transactions to the date of settlement.
- Pay Miss T £100 compensation (in addition to the £150 it has already paid).

My final decision

My final decision is that I uphold this complaint against Starling Bank Limited.

Under the rules of the Financial Ombudsman Service, I'm required to ask Miss T to accept or reject my decision before 14 June 2023.

Stephen Wise
Ombudsman