DRN-5922264

The complaint

Mr S is unhappy that Starling Bank Limited didn't reimburse him after he was the victim of a scam.

What happened

Both sides are aware of what happened so I will provide a summary.

Mr S found an advert on social media for an instant access account with an online bank (which I shall call 'Bank Z'). The account was advertised as having a guaranteed rate around 5.6% for 12 months, regardless of market conditions. There was also a £500 referral fee for referring a friend. Unfortunately, the advert wasn't genuine; Mr S was talking to scammers who had cloned the details of the genuine Bank Z.

On 21 September 2024, Mr S sent £10,000 by faster payment to what he thought was his new account. He said that he entered his own name as the payee and that the Confirmation of Payee (CoP) check couldn't confirm that the account was in his name. He also later sent £10,000 to his friend to open another account with the scammers so that he could benefit from the referral fee. This has since been refunded by another bank.

Mr S says he realised he was the victim of a scam when he kept being pressured by the scammers to refer more friends for an account. He reported the scam to Starling Bank but it declined to reimburse him. It said Mr S was required to take care before making payments which included following fraud prevention warnings and checking if a payment is genuine before sending it out.

Mr S did not agree with this outcome. He was also unhappy that Starling had arranged for an ambulance to attend his property for a welfare check. He explained that this triggered his existing vulnerabilities and caused him psychological harm. The complaint was referred to the Financial Ombudsman Service to consider.

Our Investigator looked through everything and upheld the complaint in full, but he didn't think additional compensation for distress and inconvenience was applicable in this case.

Mr S also asked our Investigator if Starling Bank could pay the costs of using a professional representative to bring his complaint. He believed Starling Bank's actions had led to him being in no psychological or functional position to be able to represent himself. Our Investigator said we wouldn't award these costs as we are a free to use service. Starling Bank disagreed with the view. It said that it had shown effective warnings and that Mr S didn't do the suggested checks on the back of this.

As Starling Bank disagreed with the view, the complaint has now come to me to make 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 may not comment on every argument raised but have focused on what I believe are the key issues to get to the heart of the matter.

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, that isn't the end of the story.

At the time the payment was made, Starling Bank had agreed to follow the Lending Standards Board's Contingent Reimbursement Model Code ('the CRM Code'). This Code required firms to reimburse customers who were the victim of authorised push payment ('APP') scams, in all but a limited number of circumstances.

Under the CRM Code, a firm may choose not to reimburse a customer if it can establish that:

- The customer ignored an effective warning in relation to the payment being made; or
- In all the circumstances at the time of the payment, in particular the characteristics of the customer and the complexity and sophistication of the APP scam, the customer made the payment without a reasonable basis for believing that:
    - the payee was the person the customer was expecting to pay;
    - the payment was for genuine goods or services; and/or
    - the person or business with whom they transacted was legitimate

However, a firm cannot decline reimbursement under the CRM Code for one of the reasons above if the customer is considered 'vulnerable'. As Mr S has argued that he was vulnerable, I have considered this first.

Was Mr S 'vulnerable' under the CRM Code?

The CRM Code states that someone is considered vulnerable to APP scams if:

"it would not be reasonable to expect that Customer to have protected themselves, at the time of becoming victim of an APP scam, against that particular APP scam, to the extent of the impact they suffered."

Mr S has shared with us his specific circumstances which he argues made him vulnerable at the time of the scam. Without going into specifics, I'm sorry to hear about the amount of loss and trauma he had been through by this point in his life.

I accept that Mr S was and is vulnerable in the plain and ordinary meaning of the word. However, I have to consider whether he was vulnerable according to the definition above. Whilst I acknowledge the points he has made, having looked through all the evidence provided, I don't think he could be considered 'vulnerable' in relation to this scam. The emails between the scammer and Mr S show that he did take steps to verify the legitimacy of Bank Z. He also clearly had some understanding about savings accounts and was confident in asking questions about the account when something wasn't clear. I also note that he had the financial intelligence to try and take advantage of the referral fee offer by asking his

friend to set up another account with Mr S' money. This suggests to me that despite everything Mr S had been through, he was able to think critically about the account and the referral offer, so he did have the ability to protect himself against this scam should any obvious red flags have appeared.

So, though I acknowledge Mr S' points, I don't think that he should be considered 'vulnerable' for the purposes of the CRM Code.

I have gone on to consider if it was fair for Starling Bank to decline reimbursement for the reasons given in the CRM Code.

Did Mr S ignore an effective warning?

Starling Bank said that Mr S' payment initiated its Payment Review Model ('PRM'), a warnings system which asks the customer a series of questions about their payment to provide a more targeted scam warning.

Mr S answered several questions and received the warning:

"##Take a moment to think A Bank or any other organisation will never tell you to move money to a new 'safe' bank account.
Fraudsters can make phone calls appear to come from a different number.
If you transfer money to a fraudster, you might not get it back.
If you're not sure the payment is genuine, stop and call us on (159)tel:159)."

Starling Bank said it also provided another fraud warning which Mr S had to acknowledge:
"Could this be part of a scam? Always verify who you are sending money to as you may not be able to recover these funds. A fraudster may tell you to ignore these warnings. Call us on 159 (or 0207 930 4450) or visit our website for scam advice."

The CRM Code gives minimum criteria for what makes a warning effective. Having considered this, I agree with the Investigator that neither warning was impactful or specific enough to meet the minimum standards expected:

- Neither warning gave Mr S an idea of the hallmarks of the particular scam that he was falling victim to so that he had a better chance of protecting himself from the scam.
- The scam warning Starling Bank provided focuses on a particular scenario typically known as a 'safe account scam' -where a consumer is being pressured to send their money in order to keep it safe, whereas Mr S was willingly making a payment without that level of pressure, so it wouldn't have resonated with him in the same way.
- The warnings don't tell a customer how to verify they are speaking to someone genuine, they simply suggest calling Starling Bank or reading Starling Bank's website, which would mean being taken to a page outside of the payment journey. This would not help Mr S assess the scam risk in the moment.

So, I don't think it was fair of Starling Bank to claim an effective warning had been given and to rely on this to deny reimbursement.

Did Mr S make the payment without a 'reasonable basis for belief'?

Having considered the evidence, I think that Mr S did have a reasonable basis for believing the scam was legitimate:

- Fundamentally, this was a sophisticated scam where a genuine bank was cloned by scammers. Mr S' checks understandably focused on confirming Bank Z existed and was authorised to operate, rather than on seeing if Bank Z was being cloned by someone else. This is why he carried out checks like looking up the bank on Companies House rather than verifying the contact details for the person he was speaking to at the cloned bank. I also note that the scammers were answering Mr S' questions with information from the genuine Bank Z, such as providing him with the legitimate Firm Registration Number (FRN') which meant that his checks would confirm that Bank Z was legitimate.

- The screenshots Mr S provided of the cloned bank look professional and persuasive and match Bank Z's branding very closely, so I don't think it was unreasonable for him to have thought it was the legitimate site.

- The scam also involved social engineering to make Mr S think he was speaking to a genuine bank. He said the scammers asked for his identification documents to carry out verification checks. This would've reassured him that the scammers were legitimate, as a person would expect a legitimate bank to do this. Starling Bank said he should have been cautious about the procedure as it didn't follow what was outlined on the legitimate Bank Z's website, but I don't think it's reasonable to expect Mr S to have known what the process should've been in such detail.

- Mr S says that he spoke to a number of different people on the phone initially when asking questions about the account opening process. I think that this would add to his sense he was talking to a legitimate bank as the involvement of multiple people would've given the impression of a busy department at the bank.

- Mr S acknowledged at the time that the rate being offered was high for a savings account, but I don't think it was such a high rate that it risked being implausible. Starling Bank itself has raised that it was possible to get this rate at the time if you were a business customer with Bank Z. So, I don't think the rate on its own was a prominent indicator that the offer wasn't legitimate.

- Starling Bank said Mr S should've looked on the genuine Bank Z's website and seen that they didn't have a social media account on the platform where he saw the advert. However, looking at Bank Z's website as it was at the time, this information is not in a prominent place on the site, and I don't think it's reasonable to have expected Mr S to go looking for this information unless he had firm suspicions that he wasn't dealing with the genuine bank, which he didn't.

- Starling Bank also said Mr S should've carried out specific security checks on the scam website to check if it was genuine, such as checking the SSL security certificate date. Whilst this may be a helpful tip for the future in helping recognise scam sites, I don't think it's reasonable for Starling Bank to have expected him to have known about these checks given their complexity. Even if he did know about them, I wouldn't expect him to have carried out these checks as he wasn't suspicious that he was talking to a cloned bank.

- Starling Bank raised that if Mr S had looked up the FRN up online, he would've seen a warning on the FCA's website about individuals having cloned Bank Z's details and the scam would've been exposed. However, Mr S claims to have called the FCA rather than looking online to check he had the correct FRN for Bank Z, so there's no reason to think he would have seen the warning online. But even if he had looked online, his primary purpose was to check that Bank Z themselves were genuine, which the page would have confirmed.

Based on the points above, I think Mr S had a reasonable basis for believing that he was paying his new account with Bank Z. I think this belief carried him through the checks that he did and meant that he reasonably rationalised any potential concerns he came across.

Starling Bank hasn't successfully argued that it has a reason not to reimburse Mr S, so I think it is fair and reasonable for Starling Bank to reimburse him under the CRM Code.

Is there anything else that Starling Bank could have done to prevent the scam?

Outside of the CRM Code, Starling Bank also has other obligations to do with protecting its customers from financial harm.

Good industry practice requires that firms be on the lookout for account activity or payments that are unusual or out of character to the extent that they might indicate a fraud risk. On spotting such a payment, the firm should make enquiries with the customer to satisfy itself that the customer wasn't at risk of financial harm due to fraud.

In this instance, Starling Bank did detect an unusual payment and their system initiated the PRM which led to Mr S answering a series of questions about the payment. However, given that the payment Mr S made was for a significant amount of money, could not be verified by the COP process and was being paid to a new payee, I think it would've been more appropriate for Starling Bank to have stopped the payment and contacted Mr S about it directly, rather than providing online warnings.

Had Starling Bank done this, it would have been able to discuss the payment with Mr S directly and would learn that it was not going to Bank Z as Mr S intended, but a different bank. I think this would have caused alarm to both Mr S and Starling Bank and the scam would have been exposed.

So even though I agree with the Investigator that Starling Bank Limited should refund the £10,000 paid, I will be recommending that the compensatory interest for the payment should begin from the date the payment was made, rather than the date the claim was made. This is because I think that Starling Bank could have prevented the scam from occurring.

Should Starling Bank pay additional compensation for distress and inconvenience caused?

I have considered Mr S' comments about Starling Bank's actions after he reported the scam, and how it impacted him.

I'm sorry to hear how traumatic the experience was for Mr S. Whilst it's clear that the incident was very distressing for him, I don't think compensation is appropriate in this instance. Deciding to make a welfare referral is a matter of judgement for the firm to make based on the information they have at the time. I think Starling Bank had enough information to conclude that a check was in Mr S' interests, so I think it was reasonable for it to arrange a check, especially as they weren't aware of Mr S' specific triggers.

Putting things right

Should Mr S accept, Starling Bank Limited should:

- Reimburse the money lost to the scam (£10,000)
- Pay 8% simple interest from the date the payment was made until the money is paid to Mr S.

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 Mr S to accept or reject my decision before 10 February 2026.

Paula Lipkowska
Ombudsman