DRN-3677759

The complaint

Mr S complains that Starling Bank Limited won't reimburse the money he lost when he fell victim to a bank impersonation scam.

What happened

Mr S received a text message saying he needed to apply for an NHS Covid pass or risk a fine. He remembers filling in his details on the link in the message and entering his payment information. Unfortunately, it was not genuine and was really sent by fraudsters 'phishing' to obtain Mr S's personal details.

On 23 December 2021, Mr S received an unexpected phone call from a number very similar to Starling's. The caller said they worked for the bank's fraud department and told Mr S his account was being hacked. Mr S says the caller knew his name, his date of birth, his bank details and how much money he had in his account. He says he was told someone was trying to steal £2,500 from his account. Mr S says that he checked his mobile banking app and saw a transaction for this amount was in process. Thinking his account was at risk, Mr S followed the caller's instructions to move his money to another account that the hacker could not access. He says he believed he was speaking to the bank because the caller knew details that only a member of the bank's staff would know.

Mr S made five payments amounting to over £13,000. Unfortunately, he wasn't really speaking to the bank. He was interacting with a fraudster who had tricked him.

Mr S realised he'd been scammed when the caller started to play a song from a well-known film soundtrack. He says the caller asked him if he liked the song, then hung up the phone. He reported it to Starling straight away. Starling tried to recover the funds that he'd sent but only £1.54 remained.

Starling considered the claim under the Lending Standards Board's Contingent Reimbursement Model Code (the CRM Code). This is a voluntary code Starling has signed up to, designed to reimburse customers that have fallen victim to a scam. The starting position under the CRM Code requires firms to reimburse customers who have been the victims of authorised push payment scams like this in all but a limited number of circumstances. Starling said it did not have to reimburse the remainder of the loss because it had sufficient fraud prevention measures in place, and because it considered Mr S had not carried out reasonable checks to confirm the payments were genuine.

Unhappy with this, Mr S complained. Starling issued its final response. It explained it was unable to refund him because it had followed its policy and guidelines.
Mr S was disappointed with the bank's position and contacted us. Our Investigator said the complaint should be upheld. She didn't think the warnings Starling gave were impactful in Mr S's circumstances as they did not do enough to bring the scam to life. She didn't think Starling had done enough to establish that Mr S had made the payments without a reasonable basis for believing he was talking to the real bank. She noted that English is not Mr S's first language and thought he would have struggled to understand the bank's information under the pressure he was put under by the caller. She pointed out that the

payments were out of character for Mr S in both value and number. She said the bank should have been alerted that he was at risk of financial harm because of how quickly the payments were being made and how quickly his balance decreased.

Starling didn't accept our Investigator's view. It felt it had given Mr S warnings targeted to this scam. It said that whilst English is not Mr S's first language, he can read English well. It pointed out that when Mr S made the payments, the account name checking service Confirmation of Payee gave a no match result which ought to have caused him concern. It added that Mr S could have checked the number that was calling him against the number on the back of his card and if he had done so, a discrepancy with the caller's phone number being one digit away from the bank's genuine number would have been noticed.

Our Investigator pointed out to Starling that Mr S did question the caller about why the money was being sent to a different account but was given a reason that would have made sense to someone that didn't know how banks work.

Starling thought its messaging about this scam risk was clear regardless of whether Mr S thought he was talking to the bank or not. As no agreement could be reached, the matter has been referred to me to decide.

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 in all the circumstances of a complaint, 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 as a consequence 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.

Starling is a signatory of the Lending Standards Board's voluntary Contingent Reimbursement Model Code (the CRM Code), which requires firms to reimburse customers who have been the victims of Authorised Push Payment ('APP') scams, like the one Mr S fell victim to, in all but a limited number of circumstances.

Starling has argued that two of the exceptions to reimbursement apply in this case. It says that Mr S ignored the effective warnings it gave during the payment journey and he made the payment without a reasonable basis for belief that the payee was the person he was expecting to pay, the payment was for genuine goods or services and/or the person or business he was transacting with was legitimate.
Having considered the facts of the case carefully, I am not persuaded either exception applies here. I will explain why.

Effective warnings

Starling says the information it presented to Mr S at the time the payments were made were effective warnings as required by the CRM Code, so it did enough to make him aware of the

risks. But I don't consider the information was impactful enough in the circumstances of the fraud to be an effective warning under the CRM Code.

Starling recognised Mr S was transferring money to an account with another bank and reviewed the first payment by asking him a series of guided questions. I accept that the on-screen questions were broadly relevant to the type of scam he was falling victim to, but I don't think they were enough to disturb this type of scam risk or that they went far enough to influence Mr S's decision making.

The information Mr S was presented with didn't set out or bring to life what a bank impersonation scam would typically look or feel like. It didn't give important contextual information that would have affected Mr S's decision to go ahead. The guided questions don't bring to life the common features of a bank impersonation scam and they don't explain the potential consequences of continuing with an irrevocable payment.

Starling explains that Mr S was presented with a further fraud warning after the guided questions at the time the new account payee details were set up. It has provided evidence from its systems to show that Mr S saw this information at the time yet continued to proceed with the transactions. But I don't think it was unreasonable for Mr S to have proceeded to make the payments even after having seen the information Starling provided. It is important to remember that Mr S was genuinely convinced he was talking to the bank's fraud department. To have a sufficient impact, the warning had to overcome that belief by breaking the spell and trust that the fraudster had been able to generate, both verbally and by their actions. I am mindful that from what Mr S has said, the fraudster was talking to him throughout the process and coaching him through what to do, which would have impacted the time and mental space Mr S had to critically challenge what was happening. The overall environment created by the fraudster, such as by making Mr S feel panicked and using his card details to set up a payment of £2,500 that he could see in his genuine mobile banking app were very powerful.

The fraud warning required Mr S to click on a link to go to the Starling website to find out more about current scams. But at the time this information didn't resonate with Mr S. I am not convinced that he ought to have recognised his own circumstances from the information that he'd been presented with. He would have needed to have doubts to click through to Starling's website for scam advice. I don't consider that including a link to information goes far enough to meet the CRM Code's requirement to provide specific, timely and impactful information that would reduce the likelihood of an APP scam succeeding.

So, I don't think the warnings Starling gave were impactful or specific enough here given Mr S's situation at the time, and I can see why they did not have a material impact on preventing this sophisticated scam.

Reasonable basis of belief

I've also thought about whether Mr S had a reasonable basis for believing the payments were genuine. I've considered what steps he took to reassure himself about the legitimacy of the situation, and whether it was reasonable for him to follow the caller's instructions and send the money.
This is a scam that hooks its victims in the moment. It creates a short-term time pressure and a fear, exploiting the trust that customers feel in the legitimate organisation and its authority. Although Starling considers that Mr S didn't make sufficient checks before making the payments, I think there is a balance to be struck. The CRM Code requires Starling to think about all the circumstances at the time of the payments, including the characteristics of the customer along with the sophistication and complexity of the scam. In doing so, I consider Starling should bear in mind the nature of this type of scam, as well as its

customer's capability to weigh up the situation they are in at that time and make an informed decision about whether to proceed with making payments.

Mr S has explained that he thought the caller was genuinely from the bank's fraud team. He's explained that the caller knew personal details about him and details about his bank account. It's more likely than not that the fraudsters obtained some of Mr S's personal information when he interacted with the phishing text message about the NHS Covid pass. The caller knew how much money Mr S had, and they knew how to use Mr S's card details to mimic a genuine payment that was immediately visible as an attempted transaction in Mr S's genuine Starling mobile banking app. In the heat of the moment, it was not unreasonable for Mr S to believe the situation and caller were genuine.

Starling has referred to certain aspects of what Mr S was being told to do and said he should have been concerned, such as when he was being asked to make payments to accounts held by other individuals at another bank. But Mr S has explained that the caller allayed his fears and gave plausible explanations for what was going on. He said: *"I asked why a different name since the account is in my name and then he told me to write my name, I filled in the information he told me, he repeatedly assured me that he was an employee of the bank and that the bank was protecting me he was with me on the phone the whole time, instructed me what to do."*

This type of fraud was designed to impact Mr S's thoughts and actions in the moment. It can be difficult for consumers to think clearly, and take steps they might otherwise take, under the kind of worry and emotional pressure Mr S found himself under at the hands of a fraudster. That's not unreasonable and the CRM Code takes into account the sophistication of the scam and the characteristics of the consumer in its design.

Starling needs to be realistic in its expectations of what constitutes 'reasonable' when understanding the level of checks, diligence and any element of social engineering which has occurred given the circumstances of the scam and the customer. I'm also mindful that an appreciation of those social engineering techniques can be more difficult to spot when you are not a native speaker of a language. Whilst Mr S's language skills mean he is able to manage everyday life, I am mindful that the fraudsters created an environment where Mr S was being coached and placed under considerable pressure, with the focus being on securing his money.

I don't consider it was unreasonable of Mr S to believe he was genuinely speaking to his bank, or that it was unreasonable for him to act on the advice he believed his bank was giving him.

Overall

Considering everything, I'm persuaded that Starling should have reimbursed the money Mr S lost to this scam under the terms of the CRM Code. I'm not persuaded that any of the permitted exceptions to reimbursement apply in the circumstances of this case.

In addition, I think that Starling ought reasonably to have done more to prevent this scam. I am mindful that when Mr S made these payments, Starling should fairly and reasonably 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). And in some circumstances, irrespective of the payment channel used, have taken additional steps, or make additional checks, before processing a payment, or in some cases declined to make a payment altogether, to help protect customers from the possibility of financial harm from fraud.

I've looked at Mr S's account statements in the months leading up to the scam. The payments Mr S made on this day were out of character for his account in both value and frequency. All of the payments were made within half an hour and rapidly drained the balance of the account. In addition, the funds went to a new payee. I think the activity stands out as being unusual and it bore the hallmarks of common types of potential fraud. I think there were indications that Mr S was at risk of financial harm and it would be reasonable to expect Starling to have intervened by contacting Mr S to ask questions about the account activity. Had it done so, I think the scam would've quickly unfolded and he wouldn't have lost his money.

The relevance of this finding is that Starling ought to have prevented the loss, rather than just reimbursing Mr S under the provisions of the CRM Code. It follows that a fair and reasonable way to put things right would be for Starling to pay Mr S interest from the date of loss, rather than the date it decided not to refund him under the CRM Code.

From what I have seen, Starling took reasonable steps to try and recover Mr S's funds, but unfortunately only £1.54 remained. I don't think there was anything further Starling could have done which would have resulted in more funds being recovered.

My final decision

For the reasons I've explained, I uphold this complaint about Starling Bank Limited.

To put things right, Starling Bank Limited should now:

- Pay Mr S a refund of the money that was lost to the scam, less the funds it has been able to recover

- The money was lost from Mr S's current account. From what I have seen in his bank statements, Mr S's current account ran with a high balance so I think the money would have most likely remained in his account but for the scam. As such, Starling Bank Limited should also pay simple interest at the underlying account rate on the refunded amount from 23 December 2021 until the date of settlement

If Starling Bank Limited considers that it's required by HM Revenue & Customs to deduct income tax from that interest, it should tell Mr S how much it's taken off. It should also give Mr S a tax deduction certificate if it asks for one, so he can reclaim the tax from HM Revenue & Customs if appropriate.

Under the rules of the Financial Ombudsman Service, I'm required to ask Mr S to accept or reject my decision before 14 June 2023.

Claire Marsh
Ombudsman