DRN-4623098

The complaint

Mr B is unhappy that Starling Bank Limited won't reimburse him after he fell victim to a scam.

What happened

In June 2023, Mr B received a text message claiming to be from Starling, this message asked him to confirm if he had attempted to make a payment to an online retailer. Mr B responded to the message to say he had not made the payment, and then received a call from someone claiming to be from Starling. They told him that his account was at risk and that he needed to take prompt action to protect his money. Unfortunately, this call had not come from an employee of Starling, but a scammer.

The scammer told Mr B that he needed to move his money to a "safe account" and that one had already been created for him – in the name of the customer adviser who would be handling the issue – with a third-party bank. That third-party has no connection to Starling, but the scammer told Mr B that the two banks worked together.

Mr B authorised two payments to this account through the Starling app. A warning was displayed initially which asked Mr B to consider whether the payment could be part of a scam (and included a link to scam information on Starling's website), this warning said that customers should always verify who they are sending money to and that fraudsters may tell them to ignore such warnings.

Mr B continued with the payment, for £917.17, and then a few minutes later initiated a second payment, for £694.11. This second payment was flagged by Starling's systems for further checks, and Mr B was then presented with a warning, asked a series of questions about the reason for the payment, and then presented with a final warning before he confirmed he wished to proceed with the payment.

Mr B says that the scammer seemed to know which questions were being displayed at each point during the process which affirmed his belief that he was genuinely dealing with an employee of the bank. He says she was talked through how to answer the questions Starling asked.

Once Mr B realised that he'd fallen victim to a scam, he notified Starling. It looked into things but decided to not reimburse him. It considered his complaint by applying the terms of the Lending Standards Board's Contingent Reimbursement Model ("CRM") Code. It said that it had presented Mr B with effective warnings during the payment process which addressed the type of scam that he'd been targeted by. It also said that it did not think Mr B had a reasonable basis for believing that he was dealing with a legitimate representative of Starling when making the payments.

Mr B disagreed, so he referred his complaint to this service. It was looked at by an Investigator who upheld it. The Investigator didn't think that the warnings displayed during the payment process met the code's definition of an "effective warning." They were also

persuaded that Mr B had a reasonable basis for believing that the payments he was making were legitimate.

Starling disagreed with the Investigator's view. It maintained that the warnings it gave were relevant to Mr B's situation and suitably impactful. Starling also continued to argue that Mr B did not have a reasonable basis for belief given some of the features of the scam.

As Starling disagreed with the Investigator's view, the complaint has been passed to me to consider and come to 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 customer made a 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 Lending Standards Board's Contingent Reimbursement Model code ("the CRM code") is of particular significance here. It requires its signatories to reimburse customers who are victims of scams like this one, unless some limited exceptions apply, and Starling is a signatory of the Code. Starling says that one or more of the relevant exceptions are applicable in this case.

Specifically, Starling has said that:

- Mr B made payments without having a reasonable basis for believing 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 with whom he transacted was legitimate.
- Mr B ignored what the CRM Code refers to as an "Effective Warning" by failing to take appropriate action in response to such a warning.

I've considered the facts of this case carefully and I'm not persuaded that either exception is applicable here.

I'm satisfied that Mr B made these payments with a reasonable basis to believe that they were in response to a legitimate request from Starling. The scammers knew enough to instil a false confidence in Mr B that he was genuinely speaking to his bank. They knew the balance of his account and were able to accurately identify a legitimate payment Mr B had recently made. Mr B has also told us that the scammers seemed to know what he was seeing at each stage of the payment process, further convincing him that he must be speaking to a legitimate representative of the bank. I acknowledge that the call Mr B received was from a withheld number, but I don't think that would have been enough to give Mr B pause for thought, it is not uncommon for legitimate institutions to sometimes use withheld numbers.

All the actions Mr B subsequently took must be seen in that context – i.e. that he sincerely believed he was following the instructions of Starling's fraud team. Starling has pointed to certain aspects of what he was being asked to do that it thinks he should've regarded with greater suspicion. For example, the fact that he was being asked to make payments to an account held with another bank or that the account appeared to be a personal account in the name of a specific individual.

But these things were explained by the scammers. The explanations that they gave carried more weight because Mr B had already been persuaded that this genuinely was a call from Starling's fraud team. I've already explained that I don't think Mr B was careless in believing that he was genuinely speaking to his bank, so I don't think I can reasonably say that he was careless for acting on the advice he believed the bank was giving him.

I'm also not persuaded that the warnings given during the payment process were enough to undermine the reasonableness of Mr B's belief that this was a legitimate request from Starling. The initial warning given to Mr B when he set up the first payment was generic, and required him to click out of the message by following a link to see any detailed information about scams. The second set of warnings, relating to the second payment, were more detailed – including content that was relevant to Mr B's situation – such as that he should be wary of anyone guiding him through the payments, that someone telling him to make the payments would be a scammer, and that Starling would never ask him to move money to a 'safe account'.

If Mr B had been given the time to have taken on board the content of the warning and process it, I'd have expected it to have an impact on his decision making. However, for the warning to be impactful, Mr B needed time and mental space to process what the warning said. And that is one of the difficulties when attempting to prevent a scam like this. The approach of the fraudsters was to stop Mr B from pausing to think about what he was doing. I can see from the technical evidence supplied by Starling that the time between the first warning appearing on screen and the first question related to the payment being posed was less than 20 seconds. And the entire process of seeing the first warning, answering the questions, and then being presented with the second warning, appears to have taken in the region of only 2 minutes. In addition to that, Mr B's testimony is that he was coached through what to do at every stage. And the nature of this type of scam means that the scammers had created a panicked state of mind in Mr B making it considerably more difficult for the warning to be impactful.

This is a known tactic for scammers when trying to reduce the impact of warnings on a customer's decision-making process. Having apparently identified that there was a meaningful risk of Mr B falling victim to a safe account scam, the warnings needed to take into account the likelihood that the scammers would attempt to reduce its impact in this way, and I'm not satisfied that they did. So the way the scammers coached Mr B through the process meant that he didn't take on board the contents of the warnings he saw. The fact that he didn't do so means that these warnings can't have affected the reasonableness of his belief here.

So, in summary, I don't consider that Starling can reasonably rely on the exceptions it has detailed. It follows that I consider Starling should refund the payments made as part of this scam as per the CRM Code.

Putting things right

To resolve this complaint Starling should:

- Refund the payments made as a result of this scam; and
- Pay 8% interest on that amount from the date the claim was declined to the date of settlement.

My final decision

For the reasons I've explained, I uphold this complaint. Starling Bank Limited should put things right in the way I've set out above.

Under the rules of the Financial Ombudsman Service, I'm required to ask Mr B to accept or reject my decision before 4 April 2024.

Sophie Mitchell
Ombudsman