DRN-4629985

The complaint

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

What happened

In June 2023, after falling victim to a phishing text, Mr C got a call claiming to be from Starling. He was told that, due to the phishing text, payments had been attempted using his card, and that someone had gained access to his online banking meaning that his Starling account was compromised. He was told 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 C that he could either open a new account himself to move his money to or – and he was told this would be more secure – he could move his funds to several different 'encrypted' accounts which had been opened by various members of the security team.

Mr C authorised five payments to these various accounts through the Starling app. A warning was displayed each time he set up a new payee which asked Mr C 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 C was also asked questions via the app on several of the payments – and a number of payments were declined by Starling, apparently because of the answers given – and shown another warning before he confirmed he wished to proceed with the payments. Mr C says that the scammer talked him through this process, telling him what to do at each stage.

Once Mr C 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 C 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 C had a reasonable basis for believing that he was dealing with a legitimate representative of Starling when making the payments.

Mr C 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 C 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 C's situation and suitably impactful. Starling also continued to argue that Mr C 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 C 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 C 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 C 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 C that he was genuinely speaking to his bank. They referred back to the phishing text he had fallen victim to and used this as a plausible explanation for how his account might have been compromised. And Mr C says they took him through a security process which seemed similar to Starling's genuine process. I acknowledge that the call Mr C received was from a withheld number, but I don't think that would have been enough to give Mr C pause for thought, it is not uncommon for legitimate institutions to sometimes use withheld numbers.

All the actions Mr C 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 accounts held with other financial institutions or that those accounts appeared to be personal accounts in the name of various specific individuals.

But these things were explained by the scammers. The explanations that they gave carried more weight because Mr C 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 C 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 C's belief that this was a legitimate request from Starling. The initial warning given to Mr C when he set up each payee was generic, and required him to click out of the message by following a link to see any detailed information about scams. The second type of warning, which he received on one of the successful payments and on several of the declined payments, was more detailed – including content that was relevant to Mr C'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 C 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 C 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. I can see from the technical evidence supplied by Starling that each time this warning was presented, 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 one minute each time. So, Mr C didn't spend much time looking at the warnings. And he has also told us that he was coached through what to do at every stage of the process. We know from experience that in cases like this the scammer will tend to try to prevent the consumer from pausing to think, and will also try to create a panicked state of mind in the consumer, 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 C 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 C 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.

In any case, I also consider that – aside from its obligations under the Code – Starling should also have done more to protect Mr C from falling victim to this scam. Overall, taking into account the law, regulators' rules and guidance, relevant codes of practice and what I consider to have been good industry practice at the time, I consider Starling should fairly and reasonably have been monitoring accounts and any payments made or received to counter various risks, including preventing fraud and scams.

And, looking at the payment history here, I consider that by the time of the third successful payment Mr C made to the scam, Starling should have been on notice that something potentially untoward was happening, and therefore should have contacted Mr C directly to ensure he was not at risk of financial harm.

I say this because this was the third large payment – in the context of Mr C's usual spending – in one day to new payees. And while the value of these payments might not have been enough to be cause for concern on their own, I'm mindful of the fact that between these payments there had been repeated payments declined by Starling, apparently because of the answers Mr C gave to questions he was being asked in the app. Overall, I think this emerging pattern should have caused Starling concern. And it's likely that if Starling had

intervened directly at that stage – and insisted on direct contact from Mr C before allowing any further payments to go through – then further payments to the scam could have been prevented.

I've also thought about whether Starling could have done anything more to recover Mr C's funds once it was notified of the scam, but I'm satisfied Starling did what it could. It contacted the recipient banks within a reasonable timeframe, but unfortunately no funds remained by that time.

So, in summary, I don't consider that Starling can reasonably rely on the exceptions it has detailed. I also consider that Starling could have done more to protect Mr C – by contacting him directly – by the time of the third successful payment he made to the scam. 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
- For the first two payments made to the scam, pay 8% simple interest per year on that amount from the date the claim was declined to the date of settlement: and
- For the third, fourth and fifth payments to the scam, pay 8% simple interest per year on that amount from the date of each payment to the date of settlement.
-

My final decision

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 C to accept or reject my decision before 17 April 2024.

Sophie Mitchell
Ombudsman