DRN-4055482

The complaint

Mr P is unhappy Starling Bank Limited ("Starling") won't refund the money he lost as the result of a third-party scam.

What happened

I'm not going to cover all the points raised in detail. The view of 14 December 2022 covered the detailed timeline of the transactions and the details of Mr P's testimony. But, in summary in October 2021, Mr P received a message and a call which appeared to be from his other bank's fraud team. Having checked the numbers - which appeared genuine - he called back and was put through to who he thought was the fraud department but who, ultimately, turned out to be a scammer. The scammer persuaded Mr P that his account was under attack and he needed to move his money to a safe place. Mr P moved all his money to his Starling account and on from there (via eight separate transactions totalling £11,231.56) to the scammer's account. Shortly after, Mr P realised he'd been the victim of a scam and reported it to Starling.

Starling felt that Mr P had been provided with an effective warning when making the payments and said he hadn't conducted sufficient checks before proceeding. It also felt it took appropriate steps to try and recover Mr P's funds when he reported the scam, but the funds had already been removed.

Our investigator upheld the complaint from the first transaction onwards. She felt that Mr P had a reasonable basis for belief and that he didn't ignore an effective warning.
Starling didn't agree – it said that although it could see why Mr P had a reasonable basis for belief – it felt its warning was effective. It didn't think any vulnerabilities Mr P had affected Mr P's capacity to protect himself from the scam.

As the case couldn't be decided informally, it's been passed to me for a 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.

Having done so, I agree with the investigator, broadly for the same reasons.

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; regulatory rules, guidance and standards; codes of practice; and, where appropriate, what I consider to have been 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 it to make, in accordance with the Payment Services Regulations and the terms and conditions of the customer's account.

But, 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.

When thinking about what is fair and reasonable in this case, I've considered whether Starling should have reimbursed Mr P in line with the provisions of the Lending Standards Board's Contingent Reimbursement Model (the CRM Code) it has signed up to and whether it ought to have done more to protect Mr P from the possibility of financial harm from fraud.

There's no dispute here that Mr P was tricked into making the payments. He thought he was speaking to his other bank's fraud department, and this wasn't the case. But this isn't enough, in itself, for Mr P to receive a full refund of the money under the CRM Code.

The CRM Code

Under the CRM Code the starting principle is that a firm should reimburse a customer who is the victim of an APP scam, like Mr P. The circumstances where a firm may choose not to reimburse are limited and it is for the firm to establish those exceptions apply. They are:

- the customer ignored an 'effective warning' by failing to take appropriate steps in response to that warning; or

- 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 good or services, and/or that
  - the person or business with whom they transacted with was legitimate.

There are further exceptions within the CRM Code, but they do not apply in this case.
The CRM Code also outlines the standards a firm is expected to meet. And it says that when assessing whether the firm has met those standards, consideration must be given to whether compliance with those standards would have had a material effect on preventing the APP scam that took place.

I am also mindful that when Mr P made these payments, Starling should fairly and reasonably also 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 made additional checks, before it processed a payment, or in some cases declined to make a payment altogether, to help protect customers from the possibility of financial harm from fraud.

Did Starling meet its obligations under the CRM Code?

The CRM Code says that effective warnings should be risk based and, where possible, tailored to the APP scam risk indicators and any specific APP scam types identified through the user interface with which the customer is initiating the payment instructions.

I don't think Starling ought reasonably to have identified a risk with the individual payments Mr P made – given the sums involved. And so, I don't think Starling was required to provide an effective warning under the CRM Code, or that it has failed to meet its obligations under the CRM Code by not doing so.

That said, Starling says Mr P was provided with an effective warning at the time he set up the payee details. It has provided us with the actual wording Mr P saw, along with a video sample of how a warning similar to this would have been visually presented.

Did Mr P ignore an effective warning?

I appreciate the warning was relevant to the scam which Mr P fell victim to, but I don't think this warning is effective – especially in the context of the circumstances of a safe account scam. Visually it's not an impactful warning. There's a lot of text within the warning, which during a safe account scam could be difficult to follow. The warning is also not particularly direct, personal or clear which is essential in a safe account scam – particularly so given the level of coaching that's often involved in this type of scam and the fact the consumer genuinely thinks they are speaking to the bank.

I also don't think the explanation of spoofing is clear enough. I don't think it really gets across the point, that scammers can make phone numbers look like *the genuine bank's phone number* or *a very similar one* - which is a common safe account scam feature. It also puts the onus back on the consumer to identify whether it's a scam by saying 'if you're not sure the payment is genuine' when in fact, it should be more direct in confirming that such scenarios are highly likely to be or will be a scam.

Overall, I don't think the warning was effective – so I don't think Mr P ignored an effective warning.

Did Mr P make the payments without a reasonable basis for belief?

Starling seems to have accepted the investigator's conclusion on this aspect of the CRM Code but for completeness, I agree with the investigator and broadly for the same reasons.

Mr P says he received a text message from a number which appeared to be from his other bank's fraud team. Mr P says he searched the number on the internet and found that the number was his other bank's genuine telephone number and was also the telephone number which appeared on the back of his debit card.

Mr P says he then received a telephone call from a different number that also looked like another genuine telephone number belonging to the bank. He says he did not answer that call but, after checking things out, called them back. Mr P says the number he called had an automated message which confirmed he had been put through to the bank's fraud team. I've seen the numbers he was contacted by and can see they were made to look like the bank's genuine contact numbers. I think all of this reassured him he was speaking to the genuine bank.

I appreciate to the trained eye and with the benefit of hindsight, there may have been some 'red flags' but I have thought carefully about what it is realistic to have expected Mr P to do bearing in mind the pressure he would have been under in the moment of the call like this. On balance, I believe that it was difficult for Mr P to think clearly in the moment and once in the call he had little opportunity to make further enquiries. In all the circumstances, I don't think his response was unreasonable.

Should Starling have done more to try and prevent the scam and protect Mr P?

As well as the CRM Code, a bank still has wider obligations and a duty to protect its customers, as far as is reasonably possible, against the risk of financial harm from fraud and scams. As such, there are circumstances where it might be appropriate for a bank to take additional steps or make additional checks before processing a payment to help protect its customers from the possibility of financial harm from fraud.

I'm not going to go into detail here because under these considerations, I would still reach the same overall conclusion as I have under the CRM Code. That is, I would still expect Starling to refund the transactions in full. In terms of the outcome here the only relevance of this point is in respect of the date from when interest should be paid on any refunds.
I don't think the first two transactions would have caused Starling any concern. The payments were relatively small (although I appreciate it is a lot of money to Mr P) and did not look unusual or suspicious based on the account activity. Banks can't reasonably be involved in every transaction. There is a balance to be struck between identifying payments that could potentially be fraudulent and minimising disruption to legitimate payments. But I think when Mr P made a second transfer 11 minutes after the first and then a third transfer happened two minutes after that, Starling ought to have been concerned that a pattern was emerging synonymous with safe account scams. The first transfer had also been proceeded by a large credit into the account and the recent historical activity on the account was minimal. I think this looked unusual and suspicious. Starling ought to have been concerned and intervened by stopping the third transfer until it could speak to Mr P. I think if it had done - it would have broken the spell by bringing to life what this type of scam looks and feels like.

Did Starling do enough to recover Mr P's funds?

In light of my conclusions above, it is not necessary in this case to consider whether the bank also exercised enough care and urgency in trying to recover the stolen funds from the payee bank before they were irretrievably removed by the scammers. But for completeness I've also thought about whether Starling took reasonable steps to recover Mr P's funds once it was made aware he was the victim of a scam. The first scam payment was made at 17:05 on 5 October 2021 and the last payment at 18:58. The scam was reported at 21:08 and Starling contacted the beneficiary bank at 22:33 the same day. The beneficiary responded to Starling saying no funds remained and I've seen the evidence that all but 58p was removed within half an hour of the last transaction. This is not unusual as scammers usually remove funds within minutes or hours. From what I've seen Starling have done what it should've to try and recover the funds for Mr P but have been unable to obtain a refund for him.

Putting things right

In order to put things right for Mr P, Starling Bank Limited should:

Refund all the transactions

To compensate Mr P for being deprived of the money he lost, Starling should add simple interest[1] at the rate of 8% per annum to the above on the following basis:

- from the date his claim was declined to the date of settlement for transactions 1-2
- from the date of transfer to the date of settlement for transactions 3-8

[1] If Starling is legally required to deduct tax from the interest it should send Mr P a tax deduction certificate so he can claim it back from HMRC if appropriate.

My final decision

My final decision is that I uphold this complaint and I requite Starling Bank Limited to put things right for Mr P as set out above.

Under the rules of the Financial Ombudsman Service, I'm required to ask Mr P to accept or reject my decision before 21 November 2023.

Kathryn Milne
Ombudsman