DRN-4608058

The complaint

Ms A complains that Starling Bank Limited (Starling) has declined to refund payments she made as part of a scam.

The complaint

In June 2023, Ms A received a message via a messaging app, which appeared to be from her daughter.

This message contained a link which redirected Ms A to a new chat with a number that was different to her daughter's existing number. Here, the other party, who Ms A believed to be her daughter, explained that their phone had broken and that this was her new number.

After some conversation about their day, it was explained to Ms A that her daughter's online banking had been blocked because of the issues with her phone. Because of this, she asked Ms A to make a payment on her behalf and advised she'd repay her within the next couple of days.

While processing the payment, Ms A asked her daughter for her assistance as Starling were asking questions as to the purpose for which it was being paid. Ms A was advised to tell Starling the payment was to a friend and proceeded on that basis.

After sending confirmation that the payment had been made, Ms A's daughter requested a further payment. It was at this stage that Ms A grew suspicious that this was a scam and refused to make any additional payments.

Ms A called Starling to make them aware she'd fallen victim to a scam. Starling subsequently contacted the receiving bank in an attempt to recover Ms A's funds, but this was unsuccessful.

Starling investigated the matter and determined that they had sufficient fraud prevention measures in place and Ms A didn't take reasonable steps to check if the payment was genuine. Unhappy with this response, Ms A referred her complaint to our service.

An investigator looked into Ms A's complaint and upheld it, recommending Starling refund Ms A in full along with interest on this refund.

While Ms A agreed with the investigator's opinion, Starling disagreed. Starling maintained that Ms A failed to take appropriate actions following the warning they presented to her during the payment journey and that she didn't take reasonable steps to check if the payment was genuine. Starling also feel as though there were enough warnings signs in the correspondence with the scammer, meaning that Ms A didn't have a reasonable basis for believing that they were paying someone legitimate.

As the case couldn't be resolved it was passed to me to review.

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.

Starling are a signatory of the Lending Standards Board's Contingent Reimbursement Model (CRM Code) which requires firms to reimburse customers who have been the victims of APP scams like this in all but a limited number of circumstances. Starling says two of those exceptions apply in this case.

Under the CRM Code, a bank may choose not to reimburse a customer for a number of reasons. In this case, Starling has relied on the following exceptions in the CRM Code in order to decline her claim:

- The customer ignored what the CRM Code refers to as an "Effective Warning" by failing to take appropriate action in response to such an effective warning.
- The customer made payments without having 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.

When Ms A set up the new payee to pay who she thought was her daughter, Starling say they presented her with the following warning:

'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. Visit our website for scam advice.'

The underlined section in the warning contained a link to Starling's website which provided further information to current scams.

Staling haven't confirmed whether Ms A followed the link for further information relating to current scams, but have explained that Ms A was asked a number of questions prior to releasing the payments. Following these questions, Ms A was presented with the following 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 (…). By tapping 'Make Payment', you agree that you understand this warning and would like to continue with this payment.'

Ms A agreed to make the payment following this warning.

Having considered both warnings, I'm not satisfied that they meet the definition of effective warnings as set out in the CRM Code.

Neither warning includes any information about the type of scam Ms A was falling victim to. The final warning shown to Ms A relates to scams in which victims are tricked into sending their funds to a 'safe' account – which isn't relevant to the scam she was falling victim to. Because of this, I can't say that the warnings were specific to the scam Ms A was falling victim to or impactful in the circumstances.

I've considered Starling's contention that Ms A failed to take appropriate actions following the warnings presented to her. Given neither warning gives any indication as to how Ms A

may have, or ought to have, uncovered the scam, I don't think it's reasonable to suggest that Ms A failed to take appropriate action following the warnings.

Starling has also argued that Ms A failed to correctly answer some of the questions which were asked in lead up to the above warnings. Having reviewed the answers given, I can't say that Ms A deliberately set out to deceive Starling in the manner in which she answered the questions. The payment purpose was correct and the and the subsequent answers were reasonable given that Ms A thought the payment was to a genuine friend of her daughter.

Taking everything into account, I think the answers selected by Ms A appear to be similar, or as close as possible, to what she understood was happening and do not demonstrate that she was deliberately misleading the bank.

I can see that one of the payment screens advised Ms A that if someone is directing her on how to correctly answer the questions then she is talking to a scammer. But, in Ms A's case, she asked for help from the scammer rather than the scammer directing her from the outset. Because of this, I can understand why she didn't think the direction she was receiving meant she was falling victim to a scam.

Based on the above, I'm not satisfied that the warnings are specific to the scam Ms A was falling victim to and weren't impactful enough to have met the standard required to be considered effective as per the CRM Code.

Starling has also said they're not liable to reimburse Ms A under the CRM Code because she didn't have a reasonable basis for believing that the person she was paying was legitimate.

In this case, I'm satisfied that Ms A did have a reasonable basis for belief that the person she was paying was legitimate for the following reasons:

- Ms A received a link from her daughter's genuine number which led her directly to a new conversation within the messaging app on the number belonging to the scammer. Though Ms A is unable to supply a copy of this link, she has explained that it contained her daughter's name and gave no reason for her to think it was from a malicious source. Having reviewed the messages Ms A had with the scammer, it seems plausible that the link to the new message thread was received in the manner Ms A has described - via her daughter's genuine telephone number. I say this as Ms A initiates the conversation with the scammer on the new telephone number and I wouldn't have expected this to have happened if Ms A did not receive a link in the way she has described.
- Ms A had lent her daughter funds in the past and so, while the request was unexpected, it wasn't something so considerably unusual for her to receive to make her believe that it wasn't her daughter requesting the funds.
- The scammer gave Ms A a plausible explanation as to why she needed to make the payment; her daughter's phone was faulty and her new number meant that she was unable to access her online banking.
- Ms A received a positive response to the confirmation of payee. This means that it was confirmed that the payee name matched that of the account owner. Given that she was led to believe she was paying a friend of her daughter's, I believe this added to her belief that she was paying a legitimate person and friend of her daughter's.

From everything I've seen, I'm satisfied that Ms A had a reasonable basis of belief that the payment she was making was legitimate. Because of this, I'm not satisfied that Starling can rely on that exception as a reason not to refund Ms A.

Having considered everything very carefully, I'm not satisfied that Starling has evidenced that they can fairly apply an exception to reimbursement. Therefore, Starling should refund Ms A in full for the payment she made. Starling should also pay 8% simple interest on that refund, to account for Ms A's loss of use of those funds. This should be calculated from the date Starling declined to refund Ms A under the CRM Code, until the date of settlement.

Putting things right

To put things right Starling Bank Limited should:

- Refund Ms A in full for the payment.
- Pay interest on that refund at 8% simple interest from the date they declined Ms A's claim under the CRM Code until the date of settlement.

My final decision

My final decision is that I uphold this complaint and require Starling to reimburse Ms A as set out above.

Under the rules of the Financial Ombudsman Service, I'm required to ask Ms A to accept or reject my decision before 15 January 2025.

Billy Wyatt
Ombudsman