DRN-4766958

The complaint

Miss D is unhappy that Starling Bank Limited (Starling) won't refund the money she lost after falling victim to a safe account scam.

What happened

I issued my provisional decision on this complaint on 28 March 2024. I wanted to give both sides a chance to provide any further evidence and arguments before I issued my final decision. That provisional decision forms part of this final decision and is copied below.

What happened

On 13 July 2023, Miss D received a fraudulent smishing text message from a well-known courier claiming she'd missed a delivery. She clicked a link within the text to arrange a re-delivery and shared her Starling card details whilst doing do. She realised shortly after that this was a fraudulent text, and she cancelled her Starling bank card.

On 23 July 2023, Miss D was at home caring for her new-born baby and her young child when she answered the call from a fraudster at around 13:30. Miss D had missed a few calls from a withheld number that day, and when she eventually answered, the fraudster claimed they were calling from Starling. She says they knew her name and asked her to confirm personal details such as her date of birth. They also knew that Miss D had cancelled her Starling bank card recently.

They asked who else Miss D banked with and she revealed she also banked with Bank N, whom the fraudster said they were on live chat to at that moment, on her behalf. They asked Miss D to log into her Bank N online banking account. Miss D queried how she could tell she was speaking to Starling and the fraudster told her that if she sends an email to Bank N containing the smishing text, she'd get a confirmation of receipt which she did.

The fraudster told Miss D her account with Bank N was being accessed by a hacker from a mobile phone located in Liverpool. The fraudster told Miss D to transfer her funds from her Bank N account to her Starling account for security purposes, and they would in turn increase the security on her Starling account. Once she moved her funds into her Starling account, the fraudster told her they would create a new account for her in an alias name. They instructed her to download an app with a third-party provider (Firm V) and create an account. This enabled the use of open banking with her Starling account.

Miss D was sent a request for funds on the app with Firm V. When she clicked this, it took her to her Starling mobile banking app to make a payment to an 'alias' account in what she believed to be a random name.

The fraudster coached Miss D through using the Starling banking app. When she questioned the fraudster on the warnings she saw on her Starling app, they assured her that the money was going to her own account in an alias name, and they were protecting her account from hackers. And if Miss D didn't move her funds imminently, she'd be at risk of losing all her

money. Miss D made one payment of £4,696 at 14:10 on 23 July 2023. After the payment, the fraudster abruptly ended the call.

When Miss D contacted Bank N, she realised that she had been scammed. They told Miss D to contact Starling as that's where she'd sent her funds. Miss D reported the scam to Starling at 14:44 the same day. It contacted the bank Miss D sent her funds to at 15:26 the same day. But that bank didn't respond.

Starling declined to refund Miss D under the Contingent Reimbursement Model (CRM) Code, of which it's a signatory. The CRM Code sets out that Starling should refund victims of authorised push payment (APP) scams (like Miss D), in all but a limited number of circumstances. It said it had sufficient fraud prevention measures in place and gave Miss D an Effective Warning when she made the payment. It also said Miss D didn't take reasonable steps to check the payment was genuine. It noted:

- *Miss D took no steps to verify the caller*
- *She was called out of the blue from a private number and told to move her money which is not typical for any bank*
- *Banks wouldn't communicate with other banks via live chat, nor would Starling have knowledge of her Bank N account*
- *No bank would tell Miss D to download an app to make a payment and she ought to have challenged this and why she was moving her money to an account with no relevance to Starling or to Miss D*

Miss D referred her complaint to our service and our Investigator upheld it in part. They thought that Starling had fairly established an exception to reimbursement applies – that being that Miss D lacked a reasonable basis for believing the payment was legitimate.

However they also found that Starling failed to meet its requirements under the CRM Code, as the warning it gave Miss D was not an Effective Warning. Therefore he said that Starling ought to refund 50% of Miss D's loss and pay 8% simple interest on the refund from the date of the claim until the date of the settlement.

Starling didn't accept our Investigator's recommendations. In summary it said that the warning it gave Miss D was impactful and effective.

As no agreement could be reached, this case was passed to me to be decided.

What I've provisionally 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.

It's not in dispute that Miss D made the payment to the fraudster herself. So, in accordance with the Payment Services Regulations 2017 (PSR 2017) she is presumed liable for the loss in the first instance. However, as I've already set out, Starling is a signatory of the CRM Code.

I can see from Starling's technical evidence that the disputed payments are faster payments that were initiated with a third party provider. From what has been said and provided so far,

these faster payments went to another person and as such have the potential to be covered by the CRM Code.

The starting position under the CRM Code is that Starling ought to refund Miss D, unless it can establish an exception to reimbursement applies. Such exceptions to reimbursement include (as far as is relevant to this complaint) that Miss D;

- *Ignored an Effective Warning by failing to take appropriate actions in response to such an Effective Warning and/or*
- *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 goods or services; and/or the person or business with whom they transacted was legitimate*

In this case, I'm not persuaded Starling has fairly established either one of these exceptions to reimbursement applies. I'll explain why.

Effective Warnings

I appreciate Starling feels strongly that it warned Miss D against the scam she was falling victim to, when she made the payment. And, that this warning amounted to an Effective Warning under the CRM Code. It provided a warning at 14:11:14 which said:

> *"Be wary of anyone guiding you through these questions. Is someone telling you how to send this payment, which buttons to tap, or asking you to read this screen? If so, you're talking to a scammer – cancel this payment and call us.*
> *Starling will never ask you to move money to keep it safe.*
> *If you send money to a criminal, you could lose it all".*

Miss D was the asked a series of questions at 14:11:29 which the fraudster told her how to answer.

She then saw a final warning screen at 14:13:41 which said:

> *"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 159"*

Starling says Miss D challenged these warnings, so she did read and acknowledge them. So I've considered why Miss D moved past these warnings and proceeded with the payment.

For the avoidance of doubt, I'm not persuaded the warning amounts to an Effective Warning under the CRM Code. In order to be an Effective Warning under the Code, the warning needs to be (as a minimum) understandable, clear, impactful, timely and specific.

The very nature of a safe account scam involves the consumer believing they are talking to their bank, whom they trust, and following the bank's instructions. Therefore, any warning attempting to combat this scam, would need to be quite clear, direct and personal to be impactful enough to override what the consumer is being told by the fraudster. I don't think that's the case here.

I'm not persuaded that visually this is an impactful warning. There's a lot of text within the warning, which during a safe account scam could be difficult to follow. Starling has provided a video of how the warning screens would have appeared at the time, and whilst I can see

Miss D would have likely been shown different parts of the warning over different screens, it still remains true that all in all, there is a lot of text within the warning which can be difficult to follow whilst under pressure. And I'm mindful that the line of questioning between the first and final warning screen, diverts the attention away from the parts of the warning which are focused on safe account scams, which negatively affects the impact of the more relevant content.

I acknowledge the warning covers off coaching, and number spoofing (albeit spoofing wasn't a feature of the scam Miss D fell victim to), but I'm not persuaded it sufficiently brings to life enough of the key features of a safe account scam, such as being pressured or fraudsters seeming to know information the bank would know. So I can see why Miss D might have thought her bank was simply helping her by guiding her through the screens.

The warning 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', which left room for judgment. In fact such scenarios will likely not be genuine, so I'm not persuaded this was direct enough in order to be impactful. I'm mindful Miss D questioned the fraudster (who she thought was her bank) in an attempt verify that the payment was genuine. In response, they told her that they had completed security, proved they were from Starling using the Bank N email, and assured her that the funds were going to her own account. As the warning didn't sufficiently bring to life the key features of such scams, such as the fraudster mimicking a bank's security procedures, or knowing personal information about the consumer, this assured her that the payment was genuine and so she reasonably proceeded.

Overall, I'm not persuaded Starling has established the warning it gave Miss D was effective under the definitions of the CRM Code. Therefore, it hasn't fairly established that the exception to reimbursement applies.

Reasonable basis for belief

I'm satisfied Miss D had a reasonable basis for believing she was following Starling's instructions when moving her funds to an 'alias' account to keep it safe.

Firstly, Miss D had reason to believe her accounts were compromised. She knew she had responded to a fraudulent text message and shared her details with a fraudster because she took steps to block her card, which tells me she is not a careless individual. The fraudster also seemed to know she had cancelled her card, adding further to her belief they worked for Starling. Miss D suspects that the fraudster may have attempted to use Miss D's card after she'd shared her details, but as Miss D had taken steps to swiftly block her card, this would not have been successful. So that might be how they knew her card was cancelled. And from what we know about these types of scams, it's also possible that the fraudster managed to elicit that information from Miss D on the call through social engineering, without it being obvious to Miss D at the time.

Miss D received a response when she emailed Bank N – just as the fraudster said she would. This reassured her they were liaising with Bank N. The scammer was also knowledgeable about both the Bank N and Starling banking app, instructing Miss D to log into her Bank N app using 'biometrics' and they told her to take off her glasses, which made Miss D think they could access her online banking account. Of course this could have been entirely coincidental, but I can appreciate why, in the moment, this made Miss D believe they had access to her online banking.

I don't agree that it's uncommon for a bank to call from a withheld number. She was asked to complete partial information, much like a security check you'd go through with a genuine

bank. And I think the explanation of moving funds to an 'alias' name would have been believable to someone who isn't familiar with a bank's procedures and processes.

I've also considered Miss D's circumstances at the time of the scam call, and I'm compelled to find that this likely impacted her basis for believing the fraudster at the time.

Since the view was issued on this complaint, Miss D has shared with our Investigator that when she received the call from the scammer, she was settling her new-born baby and caring for her other young child who was around five years old at the time. Miss D's baby was born premature and spent some time in hospital after their birth, so this was a difficult time for her and her family, and with it only being eight month's post-partum she says she was not feeling 'herself' at the time or thinking straight.

To add to this, Miss D's baby was unsettled at the time and was crying as they were due a nap. Miss D's partner took their baby into another room to enable Miss D to continue with the call, and she continued to look after her other young child at the time. This was going on whilst Miss D was on the phone with the fraudster who was telling her funds were in imminent danger, and I can only imagine how difficult it would have been to focus in that moment. Whilst Miss D's baby was no longer in the room for the entire call, I have no doubt their distress was still somewhat of a distraction for Miss D whilst the call continued. Overall, I think these factors, paired with the mental and physical strain on any new parents, for example Miss D had said she had not yet resumed normal hormonal balance after having had her baby and 'wasn't in the right headspace to make a rational decision', together with the panic and pressure instilled by the fraudster at the time of the call, would explain why Miss D reasonably believed what she was told by the fraudster at the time, and why she felt compelled to follow their instructions.

Turning to the warning Starling presented, whilst I've explained why it wasn't effective under the Code, I've considered whether it ought to have impacted her reasonable basis for belief. But it remains true that given everything going on at that moment in time, it would have made it very difficult to focus and digest the online warning Starling gave Miss D – even reading it aloud to the fraudster. Given how difficult it would have been to take this information on board in the moment, whilst being pressured by the scammer, I'm persuaded Miss D still had a reasonable basis for believing she was following her bank's instructions.

I do acknowledge Starling's point that Miss D ought to have doubted being asked to download a third-party app, but for the reasons I've already explained, I think Miss D found herself in an incredibly difficult position at the time, and in light of those circumstances and all of the tricks used by the fraudster to make it appear genuine, I think it was reasonable that she believed she was being instructed to do that by a Starling member of staff. Overall as Starling has not established a valid exception to reimbursement can fairly be applied, it ought to reimburse Miss D in full in accordance with the provisions of the CRM Code, which it has signed up to.

Customer service

I understand Miss D is unhappy by the service provided by Starling. When she reported the scam, she received an unexpected call from Starling which she was reluctant to continue with, given the type of scam she fell victim to. And she was asked to resubmit her evidence which she found traumatic, having to revisit the evidence she said she'd already provided to Starling. Whilst I have no doubt this was upsetting for Miss D, I'm mindful that the majority of distress she felt was caused by the fraudster and the scam itself.

I understand Miss D feels the scam had a serious impact on her health and wellbeing. However, I'm not persuaded Starling missed an opportunity to prevent Miss D's loss and

therefore the impact she suffered. I know Miss D feels strongly that the payment was out of character an unusual for her account usage, so I've thought carefully about whether Starling failed to detect the transaction was related to a fraud or scam.

I've reviewed Miss D's statements from the six months leading up to the scam, and I can see the account wasn't frequently used. Between January and May 2023, there were a handful of transactions made each month. However I can see Miss D made a debit of £10,000 in May 2023 which cleared her account balance to £0.03. When she made the disputed payment in July 2023, she received a credit in of £4,440.43 from her Bank N account before making the disputed payment around 25 minutes later, leaving a balance of £0.69. This was not too dissimilar from the activity in May 2023.

Furthermore, Starling did ask Miss N a series of questions through its online warning and from this, it learned Miss D was sending the money to a family or friend's savings account, that she'd paid before, met in person and had not made an unexpected request of her. I think this intervention was proportionate to the risk identified in these circumstances, and I can see why Starling did not attempt further contact with Miss D, based on the answers she gave to its questions.

Overall I don't think Starling missed an opportunity to prevent Miss D from making the payment. That means it couldn't have prevented the impact Miss D felt from the scam, and ultimately, the actions of the fraudster. So I won't be asking it to pay an award for distress or inconvenience.

My provisional decision

For the reasons I've explained above, I intend to instruct Starling Bank Limited to:

- *Refund the outstanding loss in full (£4,696)*
- *Pay 8% simple interest on that amount from the date Starling declined Miss D's claim, until the date the refund is settled, less any tax lawfully deductible*

Both Miss D and Starling confirmed they agreed with my provisional decision and had nothing further to add.

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.

As both parties accepted my provisional decision and had nothing further to add, my final decision is unchanged from the provisional findings I've set out above.

My final decision

For the reasons I've explained, I uphold this complaint and instruct Starling Bank Limited to:

- Refund the outstanding loss in full (£4,696)
- Pay 8% simple interest on that amount from the date Starling declined Miss D's claim, until the date the refund is settled, less any tax lawfully deductible

Under the rules of the Financial Ombudsman Service, I'm required to ask Miss D to accept or reject my decision before 24 May 2024.

Meghan Gilligan
Ombudsman