DRN-3171153

The complaint

Mrs G is unhappy Starling Bank Limited won't refund money she was tricked into transferring to a fraudster.

What happened

In late August 2020 Mrs G received a call on her mobile phone, the caller ID showed the call was coming from another bank, that I'll call F. The caller, Mrs G says, knew information about her – such as who she banked with and her name – possibly gleaned from a fraudulent TV licence email Mrs G had completed before the scam.

The caller asked whether she'd completed a transaction at a retailer in a different city. When she said she hadn't, the caller went on to ask whether she'd had any problems with her TV licence. Mrs G confirmed that she had and the caller offered this as an explanation as to how her account details might have been obtained.

The caller explained that Mrs G's accounts were at risk and that she'd need to move her money to protect it – first to another account she held at Starling and then, once her new accounts were set up, to a new 'safe' account.

She made three payments that evening and three more just after midnight. The first and last payments went to someone Mrs G was told was the 'bank manager', the rest were sent in Mrs G's name, but to several different accounts. In total Mrs G sent £47,990.

When no money had arrived back into her account the following morning, Mrs G reported the matter to F and subsequently to Starling.

Unfortunately for Mrs G, she'd actually been communicating with a fraudster.

Starling declined to refund Mrs G. It said she should have taken more care before making the payments and ignored warnings it had provided – so it wasn't obligated to refund her under the provisions of the Contingent Reimbursement Model 'CRM Code'.

Our investigator disagreed. They thought the way the fraudsters had impersonated or 'spoofed' F's real number would have been particularly persuasive and the warnings provided by Starling wouldn't have been impactful in the circumstances. They also found that the transactions were unusual and out of character for Mrs G and Starling ought to have intervened before letting them leave her account. Consequently, they recommended Mrs G be refunded in full – minus the money that had been recovered or refunded from other parties – a total of £16,295.

Starling continued to disagree, in summary it said:

- Mrs G ought to have called F to verify the call, given how unusual the request was
- She ignored the fact she was warned that the name on the payee accounts didn't match her own

- It's unclear why the customer picked the wrong reason for her payment ('friends and family', rather than 'own account'). But the 'friends and family' option still displayed a warning that was specific to her circumstances: ".....*Are they asking you to move money due to their accounts being compromised? This is likely to be a scam, get them to verify the instructions with their bank first."*
- Contrary to the investigator's view, the account was new, with relatively limited activity – so the transactions would not have stood out as being unusual.

As no agreement could be reached the matter was passed to me for 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.

Starling is a signatory of the Lending Standards Board 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. In this case Starling argue that two such exceptions apply – that Mrs G made the payments without a reasonable basis for belief and that she ignored an 'Effective Warning'.

I am also mindful that when Mrs G 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 make additional checks, before processing a payment, or in some cases declined to make a payment altogether, to help protect customers from the possibility of financial harm from fraud.

Considering Starling's liability under the CRM Code

I've first considered whether Mrs G held a reasonable basis for belief in making the payments, taking into account whether she actually did believe what she was told and whether that belief, taking into account her characteristics, was reasonable.

Like the investigator, I find the element of number spoofing to be very persuasive – particularly to someone unaware of the possibility of the trick. That isn't to say a customer would be reasonable to follow *any* subsequent instruction – but it provides a strong initial basis for belief. As does the information that the caller appeared to know about Mrs G – including the supposed issues she'd been having with her TV licence. While in retrospect it might be easy to say that Mrs G should have spotted that the earlier fraudulent email she'd responded to and the subsequent call were both part of the same nefarious scheme – both the caller's apparent knowledge of some information about her and the way they seemingly were able to explain how the alleged fraud had happened would, I think, have been persuasive.

Starling argue that the nature of the requests was so unusual that Mrs G ought to have been on high alert and taken steps to verify the caller. While the request might have been unusual – in the sense that one presumes Mrs G hadn't received such a request in the past – the overall communication appears to have been interspersed with the kinds of requests most people would be familiar with – such as asking a customer to confirm transactions as genuine or otherwise. Though I accept that both the prolonged interaction with the bank and the involvement of more than one bank probably ought to have struck her as somewhat unusual, it doesn't necessarily follow that, to someone unaware that requests of this nature will always be scams, she was unreasonable to believe she was speaking to F.

I've thought about whether specific aspects of what transpired during the calls ought to have shaken Mrs G's belief that the caller was from F and giving her legitimate instructions.

Starling have provided evidence that Mrs G saw a message telling her that the account details she'd entered didn't match the recipient for three of the four accounts she paid. I've seen a demonstration provided by Starling showing what Mrs G would have seen.

She would have seen a message highlighted in red which said:

'*The name you entered does not match the account details at the other bank'*

A further message, in lighter grey text says:

Could this be a scam? If in doubt, stop. Learn more about avoiding fraud on our website.

The latter message appears throughout the payment journey. In order to continue with the payment despite having seen this message the user needs to tap 'skip' in the top right hand corner of the screen and then re-enter their passcode – at this point the second paragraph quoted above remains visible on the screen and is displayed just above where the passcode needs to be entered.

Unfortunately, Mrs G does not recall seeing such messages, so I don't know why she moved past them. She does say that such was her belief that she was speaking to F that she didn't feel she needed to question things. I've thought about this carefully and it seems to be that the fraudsters were familiar with the way the Starling application worked, they were able, for example, to direct her to a specific alternative payment reason presumably in order for her not to see the most relevant warning.

While wanting to avoid speculating about what might have happened, given the fraudsters apparent familiarity with the Starling application, Mrs G's compliance and the relative ease at which the warning screen can be bypassed, it's likely she was simply quickly directed past these screens by the fraudsters. This would explain why she cannot recall seeing them or questioning the fraudsters about their content.

Similarly, Mrs G is unable to explain why she chose 'friends and family' as the payment reason, other than she was told to do so.

But I don't think these actions were as a result of carelessness or indifference to what was happening but rather deference to whom she believed to be the expert trying to assist her. In following their instructions (which in hindsight were clearly designed to divert her attention away from warnings and concerns) she appears to have believed she was simply carrying out instructions in the most expedient way possible.

The warnings she did see – as I'll go on to discuss in more detail – weren't particularly relevant to her circumstances, so I don't think these ought to have shaken her believe that the caller was legitimate either.

Mrs G does appear to have questioned why one of the sort code she was paying wasn't that of her bank. She was told both banks used the same sort code. It's unclear whether the question was asked out of suspicion or inquisitiveness, but I don't think it was unreasonable for Mrs G to believe that some sort codes are shared by financial businesses, particularly as she was questioning one of the payments to a relatively new bank.

Lastly, she seems to have rationalised why the ‘bank manager’ would be receiving her money – that this person was taking responsibility for the investigation. Again, to the layperson and in the context of a call where their money appears to be at risk, I can understand why Mrs G didn’t question this further.

I’ve concluded that Mrs G’s basis for believing that she was speaking to F was very strong and I don’t think there was enough happening here that Mrs G, considering her knowledge and characteristics, ought to have realised that she was speaking to a fraudster or, at least, taken further steps to verify their identity.

So, I’m persuaded that she did have a reasonable basis for belief in making the payments.

Did Mrs G ignore an ‘Effective Warning’?

It’s undisputed that Mrs G did not see the warning most relevant to her circumstances – as she was directed to choose a different payment reason by the fraudsters. This is unfortunate in the context of preventing the scam, but I’m only able to assess the effectiveness of the warning Mrs G did see.

Most of the warning she did see didn’t apply to the particular scam she was falling victim to. The final part of the warning read:

Are they asking you to move money due to their accounts being compromised? This is likely to be a scam, get them to verify the instructions with their bank first."

This part of the warning was referring to scams of this nature – though, understandably, from a slightly different perspective which reduced the likelihood of a customer in Mrs G’s circumstances recognising that it somewhat related to their own position.

It’s notable that the warning above comes last in the list of other warnings. The previous warnings were also targeted at scams actually involving a payment to friends and family, so the reader in Mrs G’s position is likely to have found them completely irrelevant to their circumstances, making it less likely, I think, customers in Mrs G’s circumstances would keep reading the warnings.

I’m not convinced this warning goes far enough either – it doesn’t explain that requests of this nature will almost certainly be a scam. Neither does the warning explain the consequences of proceeding with the payment.

It’s also worth noting that in order to bypass the warning, the user only needs to tap ‘yes’ to the question, ‘are you sure you want to continue?’ – the warning does not ask the user whether they’ve read and understood the previous statement, neither has it asked them any dynamic questions about what they are doing.

In Mrs G’s circumstances the warning was likely to be even less impactful given, as I’ve set out, the way I think the fraudsters were managing her journey through the payment.

So, I’m not persuaded that Mrs G ignored an Effective Warning.

Should Starling have intervened to stop the payments?

Though I can see that Mrs G didn’t use her Starling account like a current account, I’m still of the view that there was enough activity on the account in the six months prior to the scam for Starling to recognise that the disputed payments were sufficiently unusual and out of

character that it ought to have intervened and questioned them in order to try and protect her from financial harm from fraud.

Had it asked Mrs G about the activity, I've seen nothing to suggest she would not have told Starling what was happening, that it would have quickly recognised that she was falling victim to a scam and that the loss would have been prevented.

The effect of this finding is limited, given I'm upholding the complaint, but it does mean that Starling should pay interest from the date of loss, rather than the date it declined the claim under the CRM Code. In relation to the interest, I understand the money that Mrs G transferred came from her savings held at F and, but for the scam, it's likely to have remained there. So, I think interest should be paid at the rate Mrs G would have achieved had the funds remained at F.

My final decision

I uphold this complaint and instruct Starling Bank Limited to:

- Refund the amount lost - £47,990, less the money that has been already recovered or refunded - £16,295.

- Pay simple interest per annum on that amount at the rate Mrs G would have achieved had the money remained at F, from the date of the payments to the date of settlement.

Under the rules of the Financial Ombudsman Service, I'm required to ask Mrs G to accept or reject my decision before 15 March 2022.

Rich Drury
Ombudsman