DRN-5937965

## The complaint

F, a limited company, complains that Starling Bank Limited ('Starling') won't refund the money they lost as the result of a scam.

Mr W, a director, brings the complaint on behalf of F.

## What happened

In August 2024, Mr W was contacted by someone who said they worked for Starling. They said that F's account had been compromised. Mr W was persuaded to transfer £18,050 from F's Starling account, to what the scammer described as a 'safe' account.

When the scammer started asking about Mr W's personal accounts, he became concerned, and the call was ended. Mr W immediately called Starling to report the fraud.

Starling looked into Mr W's fraud claim but declined to refund him, saying he didn't do enough checks on the legitimacy of the caller.

Mr W wasn't happy with Starling's response, so he brought a complaint to our service on F's behalf.

An investigator looked into F's complaint but didn't recommend that Starling refund them. The investigator wasn't satisfied that Mr W had a reasonable basis for believing the caller was genuine, so Starling could rely on an exception to reimbursement under the Contingent Reimbursement Model Code (CRM Code). The investigator believed the onscreen warning provided by Starling was appropriate.

Mr W disagreed with the investigator's opinion and asked for an ombudsman to review F's complaint. Mr W says the scammer told him to bypass the onscreen messages he saw when making the payment and Starling didn't provide a warning.

Having reviewed the case, I reached a different answer than the investigator. So, I issued a provisional decision explaining why and giving both parties a chance to respond before I issued a final decision.

## My provisional decision

In my provisional decision I said:

I've considered all the available evidence and arguments to decide what's fair and reasonable in the circumstances of this complaint.

In deciding what's fair and reasonable, I am required to take into account relevant law and regulations, regulators' rules, guidance and standards, and codes of practice; and, where appropriate, I must also take into account what I consider to have been good industry practice at the time.

In broad terms, the starting position at law is that Starling is expected to process payments and withdrawals that a customer authorises it to make, in accordance with the Payment Services Regulations (in this case the 2017 regulations) and the terms and conditions of the customer's account.

It's not in dispute that Mr W authorised these payments on F's behalf, although he did so not realising he was the victim of a scam.

Can Starling rely on an exception to reimbursement?

Starling are a signatory to the 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.

Under the CRM Code, a bank may choose not to reimburse a customer if it can establish that an exception applies. In this case Starling say Mr W made the payment 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.

I'm satisfied that Starling can rely on this exception to reimbursement, and I'll explain why. When Mr W was making the payment, he was asked a number of questions onscreen and given warnings by Starling relating to safe account scams. The screens Mr W saw and the questions he was asked – took 10 minutes to complete from start to finish.

These are some of the warnings and questions Mr W saw, with his answers in bold:

*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.*

*Question – Have you previously accessed the account you are making a payment to?* ***No***

*A common scam involves fraudsters opening a brand new 'safe account' for you to move your money to. This is so they have access to the account and can withdraw the funds.* ***I understand.***

*Have you paid this payee before?* ***No, this is the first payment.***

*What method of contact was used to provide you with these payment details?* ***Phone call.***

*Did the payee call you?* ***No, I phoned the payee using a number found from a trusted source.***

*Fraudsters often pretend to be from a genuine company or someone you know.*

*They can easily take over email and social media accounts or set up similar accounts, so contact looks legitimate.*

*They can also 'spoof' phone numbers, meaning that their call looks like it is from a different number.*

*We'd recommend calling them back on a number found on their website, to make sure you're talking to who you think you are.*

*Take a moment to think. A bank or any other organisation will never tell you to move money to a new, 'safe' bank account.*

I appreciate that Mr W was told by the scammer to ignore these warnings, but several of the warnings were relevant to the circumstances under which he was making the payments. This should've concerned him and made him question what the scammer was telling him. Also, it's unclear what security the scammer completed, or whether the scammer was able to share any personal information with Mr W. A genuine bank would have taken Mr W through security questions and would've shared some personal information with him to prove they were from Starling.

Mr W should've also been concerned about being asked to make a payment to a payee – that wasn't his name or his company's name. And he was told to say the payment reason was related to buying equipment. I can't see that Mr W questioned either of these points.

Taking all of these points into consideration as a whole, along with the information Mr W saw onscreen when making the payment, I'm not satisfied that he had a reasonable basis for believing the caller was legitimate. So, Starling can rely on this exception to reimbursement.

However, there are also standards set for firms under the CRM Code, which Starling needs to meet.

Did Starling meet the standards set for them under the CRM Code?

I've taken into account that the payment was made from F's business account, which will naturally have higher value payments than a personal account might. However, the £18,050 was the largest payment that had been made from F's account in the prior 12 months. All other payments of a similar but slightly lower value were made to one existing payee, whereas this was a new payee. Also, the payment reduced F's bank balance to below £100 which was unusual and out of character, as their balance was usually significantly above this level.

For all of these reasons, I'm satisfied that Starling should've identified an APP scam risk and were required to provide an onscreen effective warning when Mr W made the payment. I've reviewed the entire warning that Mr W was shown as part of the payment journey, and I'm not satisfied that it meets the requirements to be considered an 'effective warning'.

I say this because the explanation of 'spoofing' of phone numbers doesn't go far enough, and the warning doesn't bring to life enough key features of a safe account scam including the pressure element or scammers knowing what information and questions banks will ask for. So, I'm not satisfied that this warning was impactful in the circumstances or clear enough, to meet the requirements to be considered an effective warning.

On that basis, Starling haven't met the standards set for them and F is entitled to a refund of 50% of the payment.

As F has been without the use of these funds, they are also entitled to simple interest of 8% to be paid on the refund. This should be calculated from the date Starling declined F's claim under the CRM Code until the date of settlement.

My provisional decision was that I intended to uphold the complaint.

## Responses to my provisional decision

F responded to say they accepted my provisional decision.

Starling didn't accept the provisional decision, saying Mr W wasn't honest or transparent in answering some of the questions. If he had been, Starling say they could've have completed a manual review or called Mr W before releasing the payment.

Starling believe the warning they provided Mr W was effective, as it directly related to the scam Mr W was falling victim to.

## 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.

I've carefully considered the points that Starling has raised, but I've reached the same answer as in my provisional decision. I'll explain why.

The nature of safe account scams is that the consumer believes they are dealing with their bank. There is also a huge amount of pressure applied to the consumer, who believes that their money is in danger and, if they don't act quickly, they could lose it.

Here the scammers got Mr W to download a screen sharing application which had a header that read "X from Starling Security". Mr W didn't know that a bank would never ask him to download this type of software or that the header could be input by the scammer and couldn't be trusted. The scammer talked Mr W through each stage of the process, told him how to answer the questions and to ignore the warnings as they were calling from Starling's security team. The trust that is built by scammers in this situation is very hard to break, especially when they have the appearance of genuinely being a bank staff member.

So, while I appreciate that the warning contained certain points which were relevant to Mr W's situation and should've caused him concern, I'm not satisfied that the warning met the definition of effective. It didn't clearly explain what spoofing is and the consequences weren't impactful enough as it said Mr W might not get his funds back whereas it was likely he wouldn't get them back.

Starling say if Mr W had answered some questions differently it may've resulted in a manual review or them calling to discuss the payment. But Starling are aware that scammers often guide consumers on how to answer the questions to avoid detection, especially in safe account scams.

Mr W wasn't acting dishonestly in answering the questions, he was following the guidance he was being given, by someone he believed to be a Starling staff member.

On that basis, I'm still not satisfied that the warning meets the definition of an effective warning under the CRM Code, so Starling haven't met the standards set for them and Mr W is entitle to a refund. However, as explained in my provisional decision, I'm also satisfied that Mr W should've been concerned based on the warning he was shown and didn't have a reasonable basis for believing the caller was legitimate. So, F is entitled to a refund of 50%.

## Putting things right

To put things right I require Starling Bank Limited to:

- Refund 50% of the payment F made, which means a refund of £9,025.
- Pay simple interest of 8% per year on the refund, calculated from the date Starling declined F's refund under the CRM Code.*

*If Starling considers that it's required by HM Revenue & Customs to deduct income tax from that interest, it should tell F how much it's taken off. It should also give F a tax deduction certificate if they ask for one, so they can reclaim the tax from HM Revenue & Customs if appropriate.

## My final decision

My final decision is that I uphold this complaint against Starling Bank Limited and require them to reimburse F, as set out above.

Under the rules of the Financial Ombudsman Service, I'm required to ask F to accept or reject my decision before 8 December 2025.

Lisa Lowe
**Ombudsman**