DRN-5506390

The complaint

S complains that Starling Bank Limited hasn't reimbursed it for payments it made due to an impersonation scam.

What happened

In September 2023, S received an email it thought related to a ticket ballot it had entered earlier in the year. It followed the link to buy tickets and entered payment details twice, as the payment wasn't processing. At this time the computer started making a loud sound and S understood it had been hacked. A telephone number appeared on the screen for S to call for support, so it called this number.

After speaking to an agent, S understood that scammers had been able to access the computer and its accounts. S was then transferred to a government organisation who said they would work with it to protect their funds. S and its directors understood their funds were at risk and they were advised to move all their money into S's Starling account. The scam went on for over two weeks and during this time S was advised to open new accounts and make payments to various places, including an £11,000 payment to 'bait' the scammer.

The scam unravelled when S was asked to buy online gift cards. At this time, it became concerned and checked with the government organisation directly about what was going on. It confirmed that S was being scammed and the agent didn't work there. S complained to Starling about the payments it had made from that account.

Starling didn't uphold S's main complaint but some of the payments made due to this scam were recovered. S came to our Service and our Investigator partially upheld its complaint. Starling disagreed and asked for an Ombudsman to reconsider it.

I issued a provisional decision on this complaint in March 2025. My provisional findings were as follows:

> *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; regulators' rules, guidance and standards; codes of practice; and, where appropriate, what I consider to be good industry practice at the time.*
>
> *As S made one faster payment of £11,000 in this case, of particular relevance is the Lending Standards Board's Contingent Reimbursement Model Code (the CRM Code) or "the Code". The CRM Code requires firms to reimburse customers who have been the victims of APP scams in all but a limited number of circumstances. Starling has accepted that the payment S made falls within the scope of the Code.*
>
> *While the CRM Code offers considerable additional protection to the victims of an APP scam, it includes provisions allowing a firm to apply exceptions to reimbursement. This includes an exception to full reimbursement where the customer made a payment without a reasonable basis for believing they were paying for genuine goods or services; dealing with a legitimate person or business; or paying*

the person they believed they were paying.

Starling says this exception applies here. It says S made this payment without holding a reasonable basis for believing the caller was genuine and that this payment was being made to 'bait' a scammer. I've considered whether it would be fair for Starling to rely on this here.

I've taken into account what S has told us happened and how this scam started. It has explained about how its computer was taken over and the urgency of the situation. And how the scammer held information about S's banking that it hadn't shared. So this made it seem like the person calling was legitimate and so it needed to follow their instructions.

I appreciate how persuasive this could have been. But I think S ought reasonably to have taken some independent steps to check what it was being told before sending such a large sum. Like the steps it did take later on in the scam. While S may have called the number due to panic, I think it ought to have reflected on this and checked whether it belonged to the computer company it thought it did. And the payment in question here was made several days into the scam, so S had the chance to think about what was going on and carry out checks before sending a large amount of money out of its control. I don't agree the information it did hold was enough to be satisfied this was all genuine.

S believed the second agent it spoke to was from a large government organisation but didn't verify this. The number wasn't from the area this organisation publishes it works from. S was being asked to carry out a lot of financial activity, such as opening new credit card accounts and being asked to share the card details of these. And was directed to open a cryptocurrency account. None of which fits with the caller's original pretence of protecting S and its director's existing accounts from fraud. So, I'm not persuaded S ought to have thought this caller was legitimate.

S was also being asked to make this payment to 'bait' a scammer. But it's not clear why S would be expected to use its own money for this. I think S should've been concerned that a genuine government organisation would expect a small business to send £11,000 of its own money to help it catch an individual scammer. Especially as the concept was that this would hopefully make the criminal come into branch to be caught. This shouldn't have seemed like something a legitimate government organisation would expect someone to do.

Overall, while I've carefully considered everything S has said about why it believed the caller was genuine and so followed their instructions, on balance it is my finding that S made this payment without having a reasonable basis for believing what it did. So, I find Starling is entitled to rely on that exception to full reimbursement under the terms of the Code.

The CRM Code also sets out standards that firms are required to meet. Where these are not met, the firm may still be liable to reimburse a victim in part, even where it has been able to establish that an exception to full reimbursement may be fairly applied (as I am satisfied Starling can establish here).

Those requirements include the provision of what the Code defines as an Effective Warning when a firm identifies an APP scam risk in relation to a payment.

When S was making this payment, Starling identified a scam risk and so asked additional questions of S and provided warnings about common scams. It says it

provided an Effective Warning, in line with the provisions of the CRM Code. I have considered the evidence provided to determine whether I am persuaded it met its standards under the terms of the CRM Code in this respect. The Code sets out what the standards are, as well as how to consider these in the context of the case (SF):

> *The assessment of whether a Firm has met a standard or not should involve consideration of whether compliance with that standard would have had a material effect on preventing the APP scam that took place.*

Starling has provided a copy of the warning messages it says it presented S with. These were given when S entered the new payee details and then when it attempted the payment and was asked further questions about what it was for.

I appreciate that, in providing S with these messages, Starling took steps to provide an effective scam warning during the applicable points of the payment journey. However, despite this, I'm not persuaded it has demonstrated that the warnings met the requirements of an Effective Warning under the Code.

The CRM Code sets out minimum criteria that a warning must meet to be an 'Effective Warning' and this includes the warning being Clear, Impactful and Specific. The warnings Starling gave attempt to cover multiple, different scam types and are quite generic in nature. They covered a range of scenarios and said non-specific statements, such as "A bank or any other organisation will never tell you to move money to a new, 'safe' bank account." This doesn't give examples of 'other organisations' or what this might look like in practice. So, I don't think any of the warnings given were sufficiently impactful or specific as required by the CRM Code, to constitute an Effective Warning.

However, I have considered the complexities of the scam here and the actions S took. I accept S was subject to extensive social engineering and so it wasn't honest with Starling about what it was doing. I recognise Starling was attempting to tailor the warning it gave S based on how S answered the questions asked – and the answers given were all false. Starling has said the way S answered the questions prevented it from intervening and calling S to discuss the payment.

S was making a £11,000 payment to a new payee on an account, where the next highest payment in the previous six months was £1,000 to an existing payee in S's name. So while I accept S answered the automated questions dishonestly, looking at the payment being made here and the account activity, I consider a proportionate intervention would've been for Starling to call S regardless. So, I'm not persuaded the way S answered the automated questions alone means Starling couldn't have met its standards.

However, Starling has also said that had it called S, it doesn't believe it could have unravelled the scam. It says S would've continued to be dishonest, as S was when another bank did call it. I've carefully considered this argument, as Starling didn't call S and so we can't know how the conversation would've gone.

I accept that when one of S's director's banks spoke to her, this was about a £750 payment from her account into one of S's accounts, meaning the risk of financial harm is very different between these two payments. But her bank asks her if anyone has asked her to make this payment in any way, or not to discuss it with the bank. And she confidently answers "No, no one has done that", despite this not being the case.

Starling's payment also took place at this earlier point in the scam, so when S was still very convinced it was working with a government organisation. Considering this; the above call; and the way S completed Starlings questions about that payment – saying this was repaying a loan for a friend – I do think it's likely S would've continued to act to prevent any banks finding out what was going on. But I fully accept S behaved in the way it did because it was under the spell of the scammer and believed it must not share the true situation.

Looking at what happened with the other bank and more importantly the extensive social engineering S was under, I think S would've gone ahead with the payment even if Starling did meet the standards required of it. Starling was required to tailor any warning to the scam risk it identified from all the information S shared. And I don't consider S would've told Starling the situation it was really in, as it understood it mustn't share this with any other parties. So, this means Starling's failure to meet the standards expected of it didn't materially affect the outcome here and so, as an exception to reimbursement applies, it's not required to reimburse S under the Code.

I've then considered whether Starling's other, general responsibilities and duties as a bank, and good industry practice, means it ought to have done more and as a result could've prevented S's outstanding losses.

Most of the payments made from S's account as a result of this scam were card payments. Some of those payments have already been refunded to S, as they were recovered. I have considered whether Starling could've done more to recover the outstanding payments, but I'm satisfied it took reasonable steps in relation to this.

I'm in agreement with our Investigator that I wouldn't have expected Starling to have intervened on any of the card payments that it hasn't been able to recover. They are relatively low value and were being sent to genuine merchants. Looking at the general account activity up until this scam, the outstanding card payments aren't so out of character I'd have expected Starling to consider S was at risk of financial harm.

The only payments I would've expected it to intervene on are the £11,000 faster payment already discussed above and the second card payment to a travel money account on 20 September. This travel money payment has been refunded. And for the reasons set out above, I'm not persuaded that a call with S about the £11,000 payment would've prevented it being made. So I'm not asking Starling to reimburse S for any of the outstanding payments it lost to this scam.

I accept S has fallen victim to a sophisticated and complex scam, but for the reasons explained above, I don't intend to uphold its complaint. I don't consider S is due a refund under the CRM code or that Starling's failure to proportionately intervene on the larger payments have materially impacted the loss here.

Starling didn't respond to the provisional decision. S said it had nothing further to add. So the complaint has been returned to me.

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 neither party provided any further comments or information, I see no reason to change my provisional findings. So I'm not upholding S's complaint as Starling's failure to meet the standards expected of it didn't materially affect the outcome here – as I don't consider S

would've shared information for it to give an Effective Warning that changed S's actions, as covered in full detail in my provisional findings above. And as an exception to reimbursement also applies, as S didn't have a reasonable basis for belief when making the payment, Starling is not required to reimburse S under the CRM code. And I don't expect Starling to have prevented or been able to recover, more than it has, any of the other payments made to this scam.

My final decision

For the reasons set out above, I don't uphold S's complaint.

Under the rules of the Financial Ombudsman Service, I'm required to ask S to accept or reject my decision before 27 May 2025.

Amy Osborne
Ombudsman