DRN-4790918

The complaint

Miss R complains that Starling Bank Limited hasn't refunded her after she was the victim of a safe account scam in 2023.

What happened

Miss R holds a current account with Starling. In 2023, she recalls receiving a message in the Starling mobile app saying that there had been a data breach, seemingly affecting her bank data. Less than two hours later, she received a call purportedly from Starling.

Miss R says the caller knew some personal information about her, including her name, where she lived and where she studied. The caller mentioned transactions Miss R recognised and knew she'd made on her account.

Given this knowledge and the proximity to the message about the data breach, Miss A was convinced the caller was genuinely from Starling. However, unknown to her at that point, the caller was in fact a fraudster.

The fraudster told Miss R that there had been attempted card transactions on her account to two retailers in another country. Miss R hadn't made these payments.

The caller then told her that he could see that two phones were logged into her Starling account, one of which she was told must be the criminal who'd attempted to spend Miss R's money at the retailers. He said Miss R's account had been compromised and this meant her money was at risk. She needed to act urgently.

To protect her money Miss R would need to move funds to some specially set up accounts. She was told these had been created using random names and account details to avoid tipping off the criminals who were accessing her account. Miss R says she asked if she could send the money to her father's account instead — but was told by the fraudster that wouldn't be possible as it would simply put her father's account at risk too.

Miss R says she was very worried about her money being at risk. She needed these funds to pay for the academic term ahead. She followed the caller's instructions, believing this would protect her money. She says the caller guided her step by step through the bank's processes and knew what questions would be asked at each point. That was something she'd expect given the caller was from supposedly from the bank's own fraud team. The caller told her what answers to give, again under the guise of avoiding the supposed criminals identifying that the money was being protected from their theft.

She proceeded to make the following transactions:

Sequence	Time	Payee	Payment	Failed Payments
1	14:12	A	£999	

2	14:15	A	£700	
3	14:17	A		Payment of £500 declined
4	14:24	B	£1,200	
5	14:30	B		Payment of £1000 declined
6	14:32	B		Payment of £900 declined
7	14:36	B	£500	
8	14:40	C	£495	
Total amount lost			£3,894	

This type of scam is known as an Authorised Push Payment scam (an APP scam). At the time this took place, Starling was a signatory of the Lending Standards Board's Contingent Reimbursement Model (the CRM 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.

However, Starling declined to reimburse Miss R. It said one or more exceptions to reimbursement applied in this case. It said:

> - it had provided a warning message which told Miss R that anyone telling a customer how to answer the bank's questions was a scammer.
>
> - Miss R hadn't given it the correct information about the payments she was making, and this had impeded the bank from protecting her.
>
> - Starling didn't think the message about the data breach justified Miss R in believing the caller was from the bank or following the caller's instructions about what to input when making the payments.
>
> - The multiple payees and accounts held at other banks ought to have been a red-flag to Miss R.

Starling said these exceptions meant it was not required to refund Miss R for the money she'd lost. It didn't accept it was responsible otherwise, it had followed her instructions in making these payments.

Our Investigator reviewed the matter. He didn't agree with Starling's conclusions. He noted that the warning Starling had provided wasn't an Effective Warning under the terms of the CRM Code. Starling couldn't rely on the exception for a customer ignoring an Effective Warning because no such warning had been given to Miss R. He didn't think the bank had been able to establish that Miss R had made these payments without a reasonable basis for believing what she did. By the point of the payment labelled (4) in the table above for £1,200, the Investigator thought Starling ought to have identified a significantly heightened risk of fraud or scam due to the rapidity of the payments to new payees and the failed transactions. He said Starling should have intervened at that point and would have thereby stopped the scam.

Starling didn't accept the Investigator's assessment. I have therefore been asked to review

everything afresh and reach a final decision on Miss R's complaint.

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.

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.

In broad terms, the starting position at law is that a firm is expected to process payments and withdrawals that a customer authorises, in accordance with the Payment Services Regulations and the terms and conditions of the customer's account.

As noted above, where a payment was made as the result of an APP Scam, then the voluntary CRM Code can require the reimbursement of customers. But Starling says that one or more exceptions to reimbursement under the CRM Code can be applied to Miss R's case. Two exceptions to reimbursement potentially apply here:

- The Customer ignored Effective Warnings […] by failing to take appropriate action in response.

- In all the circumstances at the time of the payment, in particular the characteristics of the Customer and the complexity and sophistication of the APP scam, the Customer made the payment without a reasonable basis for believing that: (i) the payee was the person the Customer was expecting to pay; (ii) the payment was for genuine goods or services; and/or (iii) the person or business with whom they transacted was legitimate.

In order to rely on an exception to reimbursement, the CRM Code says Starling must have established that either one or both applies. Starling also needs to give consideration to whether the exception would have had a material effect on preventing the APP scam that took place.

These points are a finely balanced matter to determine in this case. This has not been an easy decision to reach. I recognise that Starling did take a number of steps in its efforts to provide Miss R with an appropriate warning. Viewed in the cold light of day, there were some concerning factors which Miss R didn't identify at the time.

But having carefully reviewed all of the available evidence on this complaint, including Starling's further representations made in response to the Investigator's assessment, I don't think the bank was entitled to decline to reimburse Miss R. I will explain why I think this.

Did Miss R hold a reasonable basis for believing what she did?

To reiterate, I consider this is a finely balanced question. But I'm not persuaded Starling has established it can apply the relevant exception to reimbursement.

I think the proximity of the message about a data breach is relevant. Starling argues that the message only indicated a breach of *data* - not of card details. I think that is an erroneous argument. I can see no reason why Miss R wouldn't have thought the data might include card information or even simply information that a determined fraudster could have used to attempted to make payments from her account.

Indeed, the message header was “Important message about your *card*” [my emphasis] and the message began “We’ve been informed that your card details may have been compromised following a data breach […]”. The call shortly after telling Miss R that someone had indeed used or attempted to use her card details for a purchase doesn’t seem likely to have been as unexpected or surprising as it otherwise might have. Rather it would likely seem a logical, if upsetting, consequence of such a breach.

With that message having preceded the scam, the call that followed would reasonably have seemed connected. I don’t think Miss R was at fault in thinking that. I’m persuaded by her recollections of the call that it was convincing and that there was nothing that reasonably ought to have alerted her that the caller wasn’t who they said they were.

Everything that followed needs to be considered in that context. The warning messages displayed were counteracted by the scammer’s instructions on how to proceed. Miss R followed those instructions believing she was in fact following the bank’s instructions on how to protect her money. She had been told to act rapidly to avoid losing her money. The timing on Starling’s screens (and the rapid frequency of the payments) show that the messages were only displayed for a brief time. That is consistent with the scammer pre-empting what would be displayed, and what questions would be asked, telling Miss R what to reply (as Miss R explains happened to her at the time).

Given the scammer’s urging, I find the text-based messages displayed during the payment process would comparatively have lacked impact – again I don’t think it was unreasonable for Miss R to have followed what she was being instructed to do by ‘her bank’ in the circumstances. The timings show that the warnings were on display for very brief periods only, consistent with Miss R following the instructions she was being given.

That applies equally to the messages warning a customer that anyone telling them how to answer must be a scammer and that the bank would never ask someone to move money to a new “safe account”. In the cold light of day that is a clear message. I accept that. But this was not such a situation. Miss R has explained she was very worried. She was fearful her money was at risk. By the point those messages were displayed she believed the person ‘helping her’ was an employee of the bank whose role was to stop her funds being stolen. I simply don’t think a text-based warning message in the form of the one Starling displayed would have had the same impact on Miss R at that point as the caller did.

The use of different payees and bank accounts (with different financial institutions) is also something I think that in the cold light of day might have given someone pause. But to reiterate, this was not that situation, and the speed and pressure Miss R was under persuades me she did not act unreasonably in the context of the relevant CRM Code exception. She was given an explanation for this, that on the face of it was not implausible.

I’m also conscious that the reimbursement exception specifies that I need to take into account the characteristics of the customer. Miss R, at the time, was 18. I think her relatively young age is a factor I can’t reasonably overlook. She’d only held this account for six months. Starling notes that it posts regular warnings about the risk of common scams, but with Miss R’s unarguably shorter experience of banking I don’t think she’d have had the same level of scam awareness as someone who’d been seeing multiple warnings about scams over the course of many years. And I’ve seen nothing to make me think otherwise.

This was a scam that had apparent complexity and sophistication – leveraging a proximate data breach warning message which Miss R had had the time to read and digest, serving to make the scam premise seem much more plausible to Miss R than it otherwise might have.

All considered, I don’t think it was unreasonable for her to have believed what she was being

told at the outset, or that it was unreasonable for her to have continued to believe she needed to act at pace to protect her funds. I find this reimbursement exception cannot be applied.

Did Miss R ignore an Effective Warning given by Starling in relation to one or more of the payments?

The relevant exception here requires as a starting point that an Effective Warning was given which the consumer ignored. The CRM Code defines an Effective Warning as being one that at a minimum meets a number of criteria (including that it is sufficiently specific and impactful). In addition, to be an *Effective* Warning I think it must also be one standing a good chance of preventing the type of scam it is intended to prevent.

However, safe account scams, such as happened here, are extremely difficult to prevent using a text-based warning message or messages. I don't underestimate the challenges Starling faces in this situation. Unlike a human interaction, a text-based warning would need to be sufficiently impactful that it could overcome and override what a customer might be being told at the same time by a determined scammer, whom the customer at that point believes is from the bank's own fraud team.

Here, Starling explains that it was impeded in providing a relevant warning by the incorrect payment reason that Miss R had been tricked into answering.

Unfortunately, and for similar reasons to those I've explained above, I don't think Starling gave an Effective Warning as defined in the CRM Code. It wasn't specific to the scam that was occurring. It did contain a number of relevant features, but in the context of a safe account scam I simply don't think it would be sufficiently impactful in the moment, for someone in the midst of a pressured socially engineered scam. So, I don't find that it would have been sufficiently impactful as to stand a good chance of preventing the scam.

In saying that, I agree with the bank that this was, at least in part, because of the information input by Miss R. But the exception requires that the customer ignored an Effective Warning that was given, not one that could have been given but wasn't. And I don't find Miss R was at fault for following the instructions about the payment purpose to choose in the specific circumstances that applied at the time – she had reason to do so.

Would Starling be responsible for the loss due to any of the payments besides under the terms of the CRM Code?

While I've found Starling ought to have refunded Miss R under the provisions of the CRM Code, I've considered whether I think Starling would otherwise have been responsible for the losses Miss R incurred.

While I've noted above that the primary obligation on Starling was to carry out Miss R's instructions, as a matter of good industry practice, that is not the end of the story. I consider it is fair and reasonable to expect Starling to have been on the look-out for the possibility of harm through fraud, and further, to have taken additional steps or made additional checks, before processing payments in some circumstances.

The first two payments, while not typical of Miss R's usual account usage, weren't so remarkable that I'd find Starling at fault for not having identified the risk of financial harm to Miss R though fraud or a scam.

But by the point of the third payment for £1,200, there had been a pattern of three payments in quick succession made to two payees that Miss R had never paid before. This had

followed on the back of a failed payment attempt and would account for a significant proportion of the balance of Miss R's account. She'd chosen the same payment reason for the different payees and was inputting the information and making the payments with considerable speed. That all seems relatively unusual.

This didn't match any prior pattern of usage in the account history. The account appears typically to have been used for day-to-day spending, and there were no prior instances of similar value payments to the scam payments being made in matter of minutes. The pattern seen here would be indicative of a potential fraud or a scam. In particular this matched the pattern expected for a safe account type scam, as this was.

With these factors present, I consider this payment was sufficiently unusual that Starling ought to have taken additional steps prior to processing Miss R's payment instruction. I think a proportionate response by Starling at this point would have been to contact Miss R to ask her about the context and circumstances surrounding the payment — in order to reassure itself the payment wasn't likely to lead to financial harm through fraud or a scam.

Starling did not take this step. But had it done so, I think it would quickly have become apparent that the call in-progress at that point was not in fact genuinely from her bank's fraud team and her funds were not in fact at risk. The true situation would have been uncovered and Starling would have prevented the loss she incurred from this payment (and the subsequent payments.

And similarly to the reasoning I have explained above, I don't think it would be fair and reasonable to apply any deduction here for contributory negligence. I find it is clear that up to and including the time of authorising the payments, Miss R was still totally in the dark and simply did not appreciate what she was doing or the consequences of her actions. She believed she was helping to protect her money and prevent a fraud, not facilitate it. I am satisfied there was no contributory negligence on this occasion, she was simply the unwitting and blameless victim of a clever fraudster. The bank was the professional in financial matters; Miss R was a layperson.

Interest on the sums lost, and Distress and Inconvenience

When Miss R asked Starling to provide information to her in relation to the scam, it failed to do so in line with the timescales required. I think in light of the impact on Miss R at an already distressing time, an award of £50 is fair and reasonable in the circumstances.

I do not know how Miss R would have used the funds she lost had Starling refunded her when I find it ought to have. To reflect the time she has been deprived of the money I consider it fair and reasonable that Starling should add interest at the simple rate of 8% per year up to the date of settlement.

Putting things right

For the reasons given above, I find that Miss R ought reasonably to have been fully refunded under the CRM Code. To put matters right I require Starling Bank Limited to pay Miss R:

- The full amount of the payments she made to this scam, less any amounts the bank has already been able to recover or otherwise return to her. The bank should do so within 28 days of receiving notification of Miss R's acceptance of my final decision;
- interest at the simple rate of 8% per year on the loss attributable to the first two payments (less any tax properly deductible) to be calculated from the date Starling first declined Miss R's claim under the CRM Code until the date of settlement;

- interest at the simple rate of 8% per year on the loss attributable to the remaining payments (less any tax properly deductible) to be calculated from the date Miss R of the payments until the date of settlement;
- £50 to reflect the distress and inconvenience caused by the delays in handling Miss R's subsequent requests.

My final decision

As set out above, I uphold Miss R's complaint about Starling Bank Ltd.

Under the rules of the Financial Ombudsman Service, I'm required to ask Miss R to accept or reject my decision before 25 April 2025.

Stephen Dickie
Ombudsman