DRN-4727444

The complaint

Ms S is unhappy that Starling Bank Limited won't reimburse her after she fell victim to a scam.

What happened

In September 2023, Ms S received a call which included an automated message saying that she had missed an important letter from HMRC and needed to discuss that letter to avoid potential legal proceedings. Ms S followed the instructions in the message and was put through to someone who claimed to be working for the Courts and Tribunals Service. This person told Ms S that HMRC had filed a case against her for tax fraud and that she could either settle the case now or go to court, which carried the risk of her having to pay significantly more. Ms S was aware that she had recently received a letter from HMRC at a relative's address (an address that she had used for official purposes previously) but she'd not yet had the chance to retrieve and read that letter.

Ms S was told to go to the Courts and Tribunals Service website to check the official number for that service, and was told she would be called from that number. Ms S then received a call from this number that she had identified as a legitimate phone number for who she believed she was speaking with. Unfortunately, this call had not come from an employee of the Courts and Tribunals Service, it was a scammer.

Ultimately, Ms S was convinced to make four payments to an account belonging to a third party, she was told these payments were to clear her name for various charges that had been levied against her. The scammers used remote access software and told Ms S they were watching everything she did, she was told that she could not let anyone know what was happening or she would be in more trouble as it was a live court case. Ms S says she was on the phone with the scammers for around two hours, with only short breaks in the conversation. After the scammers asked for more money Ms S spoke with friends to see if she could borrow more and at this stage she disconnected from the remote access software and responded to texts she'd had from her brother. He convinced her to question the scammers further, and when she did so they started threatening her and then hung up. At this stage Ms S realised she had been scammed, and contacted Starling to see if it could help.

Starling looked into things but decided to not reimburse her. It considered her complaint by applying the terms of the Lending Standards Board's Contingent Reimbursement Model ("CRM") Code. It said that it did not think Ms S had a reasonable basis for believing that she was dealing with a legitimate representative of the Courts and Tribunals Service when making the payments.

Ms S disagreed, so she referred his complaint to this service. It was looked at by an Investigator who upheld it. The Investigator was persuaded that Ms S had a reasonable basis for believing that the payments she was making were legitimate. They also did not consider that Ms S had failed in her obligations under the code by ignoring an "effective warning" as defined in the code.

Starling disagreed with the Investigator's view. It maintained that that Ms S did not have a reasonable basis for belief given some of the features of the scam. It also said that Ms S had given misleading answers in response to some of the questions it asked when it flagged the first scam payment as suspicious, Starling says this prevented it from providing her with an effective warning.

As Starling disagreed with the Investigator's view, the complaint has been passed to me to consider and come to 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.

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.

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. However, where the customer made a payment because of the actions of a fraudster, it may sometimes be fair and reasonable for the bank to reimburse the consumer even though they authorised the payment.

The Lending Standards Board's Contingent Reimbursement Model code ("the CRM code") is of particular significance here. It requires its signatories to reimburse customers who are victims of scams like this one, unless some limited exceptions apply, and Starling is a signatory of the Code. Starling says that one or more of the relevant exceptions are applicable in this case.

Specifically, Starling has said that:

- Ms S made payments without having a reasonable basis for believing that: the payee was the person she was expecting to pay; the payment was for genuine goods or services; and/or the person or business with whom she transacted was legitimate.

Starling has also said that Ms S' actions meant it was unable to provide her with an effective warning.

I've considered the facts of this case carefully and I'm not persuaded that any of exceptions in the Code are applicable here.

I'm satisfied that Ms S made these payments with a reasonable basis to believe that they were in response to a legitimate request from the Courts and Tribunals Service, acting on behalf of HMRC. I say this for the following reasons:

- Ms S knew she had recently received a letter from HMRC – but had not yet had a chance to read it – so the story the scammers gave her about missed HMRC correspondence matched up with what she already knew.
- The scammers called her from a number that was legitimately associated with the Courts and Tribunals Service, adding a layer of legitimacy to their conversations.
- Ms S received correspondence – sent via a messaging app – which appeared to be on HMRC headed paper.

All the actions Ms S subsequently took must be seen in that context – i.e. that she sincerely believed she was following the instructions of an official government agency. Starling has pointed to certain aspects of what she was being asked to do that it thinks she should've regarded with greater suspicion. For example, the fact that she was being asked to make payments to an account which appeared to be a personal account in the name of a specific individual, that she was asked to download remote access software and received correspondence via a messaging app, and that the correspondence she did receive had grammatical and spelling errors.

But many of these things were explained by the scammers. For example, she was told that online messaging and remote access software was needed because she was part of a live court case, and the payments being made to a third party were explained as being made to a representative of the court. The explanations that they gave carried more weight because Ms S had already been persuaded that this genuinely was a call from the Courts and Tribunals Service. And the enormous pressure Ms S was under to do what she was told meant that she likely wasn't able to consider the correspondence she received in any depth. I've already explained that I don't think Ms S was careless in believing that she was genuinely speaking to an official representative of that service, so I don't think I can reasonably say that she was careless for acting on the advice she believed they were giving her.

I'm also not persuaded that the warnings given during the payment process were enough to undermine the reasonableness of Ms S's belief that she was responding to a legitimate request. I've carefully considered Starling's comments about how Ms S's actions affected the warnings it gave, but they don't persuade me to reach a different view.

Under the provisions of the Code, an effective warning must have been (as a minimum) understandable, clear, timely, impactful and specific. And I'm satisfied Starling didn't provide an effective warning in this particular case. I appreciate the information provided on Starling's website is fairly comprehensive and does specifically cover HMRC scams. But, in order for a customer to see this, they would need to click the link provided by Starling near the start of the payment journey. The initial message that Starling says it presented to Ms S simply says that the payment could be part of a scam, and that fraudsters might tell her to ignore warnings, it then directed Ms S to its website for more detail. But, as I've explained, Ms S didn't think she was being scammed and didn't have any doubts about the payments she was being asked to make. So, this warning wasn't impactful and doesn't seem to have grabbed her attention in the way that Starling intended.

Starling says Ms S then selected that she was making a payment to 'friends and family'. And so she was given an additional warning relevant to that payment purpose, instead of a more relevant warning about scams involving paying invoices or bills. But I accept Ms S's assertion that the fraudster guided her through the payment journey and told her which payment option to select. And the warning Ms S was therefore shown was not relevant to the situation Ms S found herself in. I accept that Ms S' choice made it very difficult for Starling to give a tailored and impactful warning. It wouldn't be fair to suggest that Starling had failed to adhere to an obligation that it was never possible for it to meet. But it's also the case that, had its 'invoice or bill' warning met the definition of 'effective' under the CRM Code (that's not a finding I need to make here), it would be irrelevant because Ms S didn't see that particular warning. So, I don't find that Starling has failed in its obligation to provide an effective warning, but I also can't fairly say Ms S ignored an effective warning either.

So, the way the scammers coached Ms S through the process meant that she didn't see relevant warnings – whether they would have been effective or not, and the fact that she didn't do so means that these warnings can't have affected the reasonableness of her belief here.

In any case, I also consider that – aside from its obligations under the Code – Starling should also have done more to protect Ms S from falling victim to this scam. Overall, taking into account the law, regulators' rules and guidance, relevant codes of practice and what I consider to have been good industry practice at the time, I consider Starling should fairly and reasonably have been monitoring accounts and any payments made or received to counter various risks, including preventing fraud and scams.

And, looking at the payment history here, I consider that by the time of the third payment Ms S made to the scam, Starling should have been on notice that something potentially untoward was happening, and therefore should have contacted Ms S directly to ensure she was not at risk of financial harm. I say this because this was the third large payment – in the context of Ms S' usual spending – in around two hours, to a new payee. And while the value of these payments might not have been enough to be cause for concern on their own, overall, I think this emerging pattern should have caused Starling concern.

And it's likely that if Starling had intervened directly at that stage – and insisted on direct contact from Ms S before allowing any further payments to go through – then further payments to the scam could have been prevented.

I've also thought about whether Starling could have done anything more to recover Ms S' funds once it was notified of the scam, but I'm satisfied Starling did what it could. It contacted the recipient bank within a reasonable timeframe, but unfortunately no funds remained by that time.

So, in summary, I don't consider that Starling can reasonably rely on the exceptions it has detailed. I also consider that Starling could have done more to protect Ms S by the time of the third successful payment she made to the scam. It follows that I consider Starling should refund the payments made as part of this scam as per the CRM Code.

Putting things right

I am mindful that the payments Miss S made to the scam were funded, in part, by loans from friends and family. I am also aware that those funds have now been repaid by Ms S. As a result, to resolve this complaint Starling should:

- Refund the payments made as a result of this scam; and
- Pay 8% interest from the date Ms S repaid her friends and family for the first three payments, and pay 8% interest from the date of transaction for the last payment.

So, in simple terms, Starling should pay 8% interest on the following amounts from the stated dates:

- 20 September 2023 on £4001 of the loss
- 4 October 2023 on £1000 of the loss
- 2 November 2023 on £600
- 8 November 2023 on £400
- 14 December 2023 on £500
- 31 January 2024 on £500

To represent 8% interest from the date the funds were repaid to the lenders by Ms S for the first three payments.

And then 8% interest from 18 September 2023 on £256 to represent interest from the date of transaction for the last payment.

My final decision

For the reasons I've explained, I uphold this complaint. Starling Bank Limited should put things right in the way I've set out above.

Under the rules of the Financial Ombudsman Service, I'm required to ask Ms S to accept or reject my decision before 12 September 2024.

Sophie Mitchell
Ombudsman