DRN-4892752

The complaint

F – a limited company – complains that Starling Bank Limited ('Starling') hasn't refunded all the money it lost as the result of a scam.

Miss F has brought the complaint on behalf of F. And, for ease, as she was the individual who made the scam payments, I've referred only to Miss F throughout my decision.

What happened

The circumstances of the complaint are well-known to both parties, so I don't intend to set these out in detail here. However, I'll provide a brief summary of what's happened.

In February 2024, Miss F received an email, which she believed to be from a genuine parcel delivery company – which I'll refer to as 'E'. The email said E had been unable to deliver a parcel to Miss F, which she'd been expecting. The email contained a link for Miss F to arrange for the parcel to be redelivered. Miss F clicked the link, which prompted her to provide some personal information and bank details. Miss F entered her name, address, phone number and her bank details for her personal account with another bank – which I'll refer to as 'Bank A'. Unbeknown to Miss F at the time, this wasn't a genuine email and was a 'phishing' email, designed to obtain her personal details.

A few days later, Miss F received a call from a third party ('the first scammer'). The first scammer claimed to work for Bank A's fraud department, and they were calling because some suspicious activity had been identified on Miss F's account, including an out of character payment and a car loan application, both of which had been blocked. Miss F says the first scammer knew her name, address and bank details with Bank A. The caller also appeared to be calling from a genuine contact number for Bank A's fraud department, which Miss F verified as genuine online.

The first scammer asked Miss F if she had recently clicked a link in any emails and Miss F confirmed she had responded to an email she believed to have been sent by E. The first scammer told Miss F that the email she had received from E was actually from a fraudster and her devices were likely infected with a virus, which had given the fraudster access to all her bank accounts. The first scammer said that they would pass Miss F's details to a colleague, who would be able to help her secure her account with Bank A. Miss F was given a code to share with the next caller, as part of Bank A's "*security protocol*".

Miss F was subsequently contacted by a different third party ('the second scammer') and Miss F provided them with the code she'd been given in the earlier call. The second scammer told Miss F that they held a special licence from the FCA, which allowed them to provide support to customers who'd been targeted by fraudsters, and this allowed them to help secure accounts held outside of Bank A, including Miss F's business account with Starling.

Miss F was told that to protect her Starling account, her funds would need to be moved to a safe account within Starling and that this needed to be done in a specific way to prevent fraudsters tracing where the funds were going, which the second scammer referred to as "*masking*".

The second scammer asked Miss F to share the long card number and CVV for her Starling account, which she did. They then initiated two online debit card payments to an international money transfer service – which I'll refer to as 'W'. The second scammer asked Miss F to approve the payments via the Starling mobile app. Believing she was authorising the movement of her funds from her Starling account to a safe account within Starling, Miss F approved payments for £4,800 and £2,120, which actually went to W.

The second scammer said Miss F needed to open a new account with Bank A, so she could move her funds held with that bank. Miss F thought this was suspicious and refused to do this, at which point she discovered she'd been the victim of a bank impersonation ('safe account') scam.

Miss F contacted Starling for help. Starling didn't think the first scam payment (for £4,800) was so unusual that it reasonably ought to have been expected to have prevented the payment being made. However, Starling agreed that it could've done more to prevent the second scam payment (for £2,120) and so that payment was reimbursed.

Miss F thought the first scam payment was unusual and believed Starling could've done more to prevent it. She also didn't think Starling had handled her scam claim well enough. So, Miss F made a complaint. Starling maintained its decision not to reimburse the first scam payment, but it did pay Miss F £100 compensation because of the customer service she received.

Unhappy with Starling's response, Miss F referred her complaint to this service. Our Investigator upheld the complaint. They thought the first scam payment was unusual, compared with Miss F's typical account activity, so Starling should've done more to ensure the payment was being made for a genuine reason *before* processing it. To resolve the complaint, our Investigator recommended Starling refund £4,800 to Miss F, with interest.

Starling didn't agree. It said the first scam payment wasn't unusual at the time it was made. Whilst it was larger than the typical spend on the account, there were sufficient funds available to make the payment, it was made from a business account (where payments are typically larger in value than personal accounts) and customers do occasionally make genuine payments that are larger than normal. Starling also said it has a responsibility to its customers to approve payments without unnecessarily delaying them.

As an agreement couldn't be reached, the complaint has been passed to me to decide.

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 have been 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 (in this case, the 2017 regulations) and the terms and conditions of the customer's account.

Whilst Miss F didn't initiate the scam payments herself, it's not in dispute that she approved them via Starling's mobile app and knew funds were leaving her account. So, the payments were authorised and under the Payment Services Regulations, the starting position here is that Miss F is responsible for the payments (and the subsequent loss) despite the payments being made as the result of a scam.

However, that isn't the end of the story. Good industry practice required Starling to be on the lookout for account activity or payments that were unusual or out of character to the extent that they might indicate a fraud risk. On spotting such a payment, I'd expect it to take steps to warn the customer about the risks of proceeding.

In the seven months prior to the scam, the largest payment Miss F had made from the account was a £1,900 faster payment to an account in her own name. The value of that payment was less than 20% of the account balance at the time. She had previously made some low value payments abroad but hadn't sent funds via an international money transfer service – such as W – before.

The first scam payment was a £4,800 payment, which reduced her account balance by over two thirds. Whilst there was still over £2,000 remaining in the account, it was out of character for the balance to be reduced so significantly by a single transaction. Also, the payment was being sent abroad via W, which demonstrated a greater risk than a payment being made within the United Kingdom. The value of the payment, together with the reduction of the account balance and beneficiary demonstrated a change in the operation of the account.

I accept that business accounts do typically make larger payments than personal accounts. However, from the account statements I've seen, that isn't the case for Miss F, who hadn't made a payment exceeding £800 to a third party within the seven-month period prior to the scam taking place. I also accept that customers do, from time to time, make larger than usual payments and these payments can be for genuine reasons. However, when an out of character payment is made, I'd reasonably expect a payment service provider to take steps to verify that the payment isn't being made as a result of fraudulent activity.

Here, I'm satisfied that the first scam payment was out of character, for the reasons I've explained above. So, I think Starling reasonably ought to have been concerned that Miss F was at risk of financial harm. I'm persuaded that Starling ought to have taken steps to satisfy itself the payment was for a genuine purpose, *before* processing it.

When Miss F approved the first scam payment Starling says it showed her a warning that said:

> "***We think this payment is high-risk***
>
> *Our systems have identified this payment as a possible scam. If you send money to a scammer, you could lose it all.*"

Miss F doesn't recall seeing this warning. However, in any event, the warning didn't explain why Starling thought the payment was high-risk, nor did it provide any scam education or advice on how to spot common scam types. As a result, I wouldn't have expected this warning to have resonated with Miss F at the time.

The first scam payment demonstrated a risk of fraud and a proportionate response in the circumstances would've been for Starling to have questioned the purpose of the payment through a better automated warning. This would've allowed Starling to have narrowed down the risk demonstrated by the payment and given it an opportunity to provide some key features of common scams – such as safe account scams, as was the case here.

Miss F has said that the second scammer didn't give her a cover story. So, there was no reason for Miss F not to have been honest if questioned. If Starling had asked her questions about the payment, I think she would, more likely than not, have answered truthfully that she was moving funds to a safe account.

Had this information come to light, Starling would've been able to highlight the common features of a safe account scam, many of which were present in Miss F's circumstances. And I'm persuaded this information would've resonated with Miss F at the time. I say this because when the second scammer asked her to open a new account with Bank A, she found that this was suspicious, and she immediately ended the call and reported the situation to Starling. So, at the time the first scam payment was made, I think education and a warning about safe accounts scams would, more likely than not, have given Miss F enough doubt about what she was doing that she wouldn't have approved the transaction and the loss could've been prevented.

I accept it's possible, given the sophistication of the scam, that Miss F might have been coached by the second scammer on how to answer Starling's questions. But I'm mindful in the particular circumstances of this complaint that to bypass the questions, Miss F would've needed to have been told to lie to Starling about the reasons for making the payment. If she'd been told to lie, I think that would've, more likely than not, given her enough cause for concern that she wouldn't have proceeded to approve the transaction.

This leads me to the conclusion that Miss F would, more likely than not, have responded positively to a safe account scam warning and wouldn't have gone ahead with the payments had this happened. Starling didn't provide Miss F with a safe account scam warning and therefore missed an opportunity to prevent Miss F from losing money to the scam. So, I'm persuaded Starling can fairly be held responsible for the loss.

A few days prior to the scam, Miss F had responded to a phishing email and disclosed information about her account with Bank A. So, when the first scammer called Miss F and said they worked for Bank A, they knew information about her to corroborate this story, such as her name, address, phone number and bank account details. They were also able to spoof a phone number for Bank A, which Miss F checked online and found to be a genuine number for Bank A's fraud department. Miss F was transferred to the second scammer, who she had to disclose a code to, given to her by the first scammer, as part of a security protocol, which will have made the scam more convincing.

The first scammer gave a reasonable explanation for how her accounts had been compromised, in that by responding to the phishing email her devices had been infected with a virus. The second scammer also gave a plausible explanation for why they were able to help her move funds from her account with Starling whilst working for a different bank, by claiming they were licensed by the FCA to safeguard funds held in all Bank A's customers' accounts.

Miss F doesn't recall seeing who the beneficiary of the payment was, but I think this information was most likely shown to her on the Starling mobile app. However, at the time the payment was made, Miss F didn't recognise the name of W and she thought the payment was going to a safe account held within Starling. Looking at the payment screen, I can understand how Miss F could've been led to believe that the funds weren't leaving Starling, as she didn't recognise that W was an international money transfer service.

Taking all this information into consideration, I think Miss F was acting reasonably by following the second scammer's instructions, on the false understanding that they were helping her to keep her funds safe. As a result, I'm not persuaded Miss F can be held responsible for the loss.

Starling's customer service

Miss F has explained that she's not happy with how Starling handled her scam claim, specifically the lack of communication between reporting it and receiving an outcome.

It took Starling approximately two weeks to investigate Miss F's scam claim and give her an answer. Whilst it wasn't the answer Miss F was hoping for, I don't consider that to have been an unreasonable amount of time for Starling to take. I also don't think there was a need for Starling to have proactively contacted Miss F to give her updates during that time.

Starling has already paid Miss F £100 compensation for her complaint about its customer service. In the circumstances, I'm not persuaded Starling needs to do anything more than this in recognition of how it handled Miss F's scam claim.

Putting things right

For the reasons explained, I don't think Starling did enough to protect Miss F from fraud, nor do I think Miss F ought to share responsibility with Starling for the loss she's suffered as a result of the scam. To resolve the complaint, Starling should:

- refund Miss F's outstanding loss of £4,800 in full; and
- pay 8% simple interest per year on that amount, calculated from the date of payment until the date of settlement.

My final decision

My final decision is that I uphold this complaint against Starling Bank Limited.

Under the rules of the Financial Ombudsman Service, I'm required to ask F to accept or reject my decision before 24 April 2025.

Liam Davies
Ombudsman