DRN-5090812

The complaint

Mr K, on behalf of company W Ltd has complained that Starling Bank Limited ("Starling") failed to protect him from falling victim to an impersonation scam.

What happened

The background of this complaint is already known to both parties, so I won't repeat all of it here. But I'll summarise the key points and then focus on explaining the reason for my decision.

Whilst I've noted this complaint relates to W Ltd as the eligible complainant, I'll refer mainly to Mr K in my decision as he's the party that's referred the complaint here.

Mr K explains that in December 2023 he was contacted by an individual ("the scammer") posing to be from Starling, alerting him to some alleged suspicious transaction on his account. He explains that he was told his money would need to be moved into a safe account, and he was told by the scammer to approve two transactions totalling £8,904.90 in his Starling mobile application. Mr K says he refused to approve the transactions, but they were processed anyway. The next day Mr K reported further fraudulent transactions on his other business account with a combined value of £8,930.65.

Around two weeks later Mr K was refunded £8,904.90 on his first business account, which was made up of refunds from the merchant and from Starling.

Starling then contacted Mr K around a week later to gather some more information about the remaining disputed payments. Mr K told it he'd noticed the transaction shortly before receiving a call from someone from Starling, but he told Starling he didn't give the caller a payment code generated by the Starling app in order to authorise the payments.

After a couple of weeks Starling told Mr K it wouldn't refund the outstanding disputed transactions. It said the transactions were approved using the Online Payment Code which could only be accessed using Mr K's Starling app on his mobile phone. It said that whilst scammers may have initiated the payments from Mr K's account, Mr K must have provided them with the code from his mobile phone. And Starling said that when it gives the code it shows a warning – including that Starling will never ask for the code, and it should've never be given to a third party.

Mr K made a complaint to Starling. He complained that Starling had refunded the fraudulent payments on one of his accounts, but not the other, despite the circumstances of both being the same. Starling didn't uphold the complaint as it maintained that Mr K provided the Online Payment Code to the scammer. Mr K remained unhappy so he referred the complaint to this service.

Our investigator considered everything and didn't think the complaint should be upheld. He explained that he thought liability for the losses should be shared between Mr K and Starling. And as Mr K had already had a refund of over 50% of his total losses, the investigator didn't think Starling needed to do anything else to put things right.

Mr K didn't accept the investigator's opinion, and he asked for more information about the Online Payment Codes that were given to the scammer. As the case has now been passed to me, I'll include that information in my 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.

I'm sorry to disappoint Mr K but having considered everything I'm afraid I'm not upholding his complaint, broadly for the same reasons as our investigator, which I've set out below.

In broad terms, the starting position is that a firm is expected to process payments and withdrawals that its customer authorises, in accordance with the Payment Services Regulations and the terms and conditions of the customer's account. And in this case it's not in question whether Mr K authorised these payments from leaving his account. It's accepted by all parties that Mr K gave the instructions to Starling and Starling made the payments in line with those instructions, and in line with the terms and conditions of Mr K's account.

I've kept my decision relevant to the issue at hand here, so as to ensure the complaint can be resolved a swiftly as possible for all parties involved. That's to say, whether I think it's likely the Online Payment Codes were given to the scammer by Mr K.

Having reviewed everything, I agree with the investigator that it's likely Mr K did give the Online Payment Codes to the scammer, and that Starling has done enough to put things right – so I'm not telling it to do anything further.

Whilst there's some evidence to support that Starling could've done more to protect Mr K's in this scenario, I've also given due consideration to the part Mr K played in the scam taking place. Although I do understand Mr K was likely pressured to make heat-of-the moment decisions due to the sense of urgency created by the scammer, I'm persuaded that Mr K gave the scammer the Online Payment Codes that Starling made clear he shouldn't share with any other parties.

I've been provided with confirmation that the Online Payment Codes were generated by the mobile phone registered on Mr K's account – and that it appears Mr K did all of his other banking using. So I'm persuaded that that the Online Payment Codes originated from Mr K's mobile phone and were either entered into a website by Mr K as part of a transaction, or given to the scammer for them to do so – as they could only have been accessed on Mr K's mobile phone. This allowed the payments to be made, and therefore meant the intervention Starling had in place to prevent fraud of this nature didn't work as it was intended.

The warning shown each time an Online Payment Codes is given says:

"Never share your code - Starling will never ask you to share this code. Only tap ''Get Code" if the merchant website or app is asking for it to confirm the card purchase you're currently making. If someone is telling you to give them this code, please refuse and contact our customer service".

I do understand there may've been some confusion around the purpose of the Online Payment Codes and I'm sorry that happened to Mr K if that's the case. But in order for me to conclude that starling were responsible for that, I'd need to be satisfied that Starling's actions or inactions are what caused it. And for the reasons I've set out above, that's not the case.

In addition, although Mr K was aware of the fraudulent transactions on his first account, it appears he continued to give the scammer the Online Payment Codes, multiple times, on his second account. The payments on the second account were made after those on the first account, after Mr K says he noticed the initial ones. So I'm persuaded that Mr K could've exercised more caution before sharing the information by phone which ultimately led to the payments being made.

Taking into account the fact that one of the merchants and Starling have already refunded almost 50% of the total of what Mr K lost, and as I don't believe Starling is responsible for Mr K's losses, I don't require Starling to pay Mr K anything further to settle this complaint.

I'm very sorry that Mr K and his company have fallen victim to this scam and I do understand that my decision will be disappointing. But for the reasons I've set out above, I don't hold Starling responsible for that loss, so I don't require Starling to pay anything further to W Ltd, or Mr K, than it has already paid.

My final decision

I don't uphold Mr K's complaint, on behalf of W Ltd, against Starling Bank Limited.

Under the rules of the Financial Ombudsman Service, I'm required to ask W to accept or reject my decision before 14 January 2025.

Sam Wade
Ombudsman